Sammlung Schubert

Sammlung mathematischer Lehrbücher.

Verzeichnis der erschienenen und projektierten Bände.

Erschienen sind bis September 1907:

Band I: **Elementare Arithmetik und Algebra** von Professor Dr. Hermann Schubert in Hamburg. Geb. M. 2.80.

„ II: **Elementare Planimetrie** von Prof. W. Pflieger in Münster i. E. Geb. M. 4.80.

„ III: **Ebene und sphärische Trigonometrie** von Dr.

„ ...ohnert in

„ ..., **Wahr-** ... **und dio-** ... Hermann

„ ... **Zahlen-** ... M. 4.40.

„ ...ud. Böger

„ ... Dr. Max

„ ...**e, Ebene,** ...b. M. 4.—.

„ ...**l: Diffe-** ...Meyer in

„ ...**ntegral-** ... Königs-

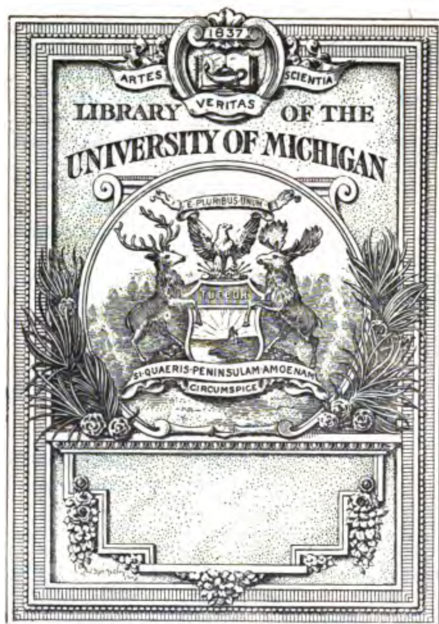
„ ...**der dar-** ...röder in

„ ...hlesinger

„ ...Runge in

„ ...**echnung** ....—.

„ ...mann in ... Wien. Geb. M. 5.—.



„ XXIII: **Geodäsie** v. Prof. Dr. A. Galle i. Potsdam. Geb. M. 8.—.

„ XXV: **Analytische Geometrie des Raumes II. Teil: Die Flächen zweiten Grades** von Prof. Dr. Max Simon in Straßburg. Geb. M. 4.40.

„ XXVII: **Geometr. Transformationen I. Teil: Die projektiven Transformationen nebst ihren Anwendungen** von Prof. Dr. Karl Doehlemann in München. Geb. M. 10.—.

„ XXIX: **Allgemeine Theorie der Raumkurven u. Flächen I. Teil** von Prof. Dr. Victor Kommerell in Reutlingen u. Prof. Dr. Karl Kommerell in Heilbronn. Geb. M. 4.80.

Band XXXI: **Theorie der algebraischen Funktionen und ihrer Integrale** von Oberlehrer E. Landfriedt in Straßburg. Geb. M. 8.50.

„ XXXII: **Theorie und Praxis der Reihen** von Professor Dr. C. Runge in Hannover. Geb. M. 7.—.

„ XXXIV: **Liniengeometrie mit Anwendungen I. Teil** von Prof. Dr. Konrad Zindler i. Innsbruck. Geb. M. 12.—.

„ XXXV: **Mehrdimensionale Geometrie I. Teil: Die linearen Räume** von Prof. Dr. P. H. Schoute in Groningen. Geb. M. 10.—.

„ XXXVI: **Mehrdimensionale Geometrie II. Teil: Die Polytope** von Prof. Dr. P. H. Schoute in Groningen. Geb. M. 10.—.

„ XXXVII: **Lehrbuch der Mechanik I: Kinematik** von Prof. Dr. Karl Heun in Karlsruhe. Geb. M. 8.—.

„ XXXVIII: **Angewandte Potentialtheorie in elementarer Behandlung I. Teil** von Prof. E. Grimsehl in Hamburg. Geb. M. 6.—.

„ XXXIX: **Thermodynamik I. Teil** von Prof. Dr. W. Voigt in Göttingen. Geb. M. 10.—.

„ XL: **Mathematische Optik** von Prof. Dr. J. Classen in Hamburg. Geb. M. 6.—.

„ XLI: **Theorie der Elektrizität und des Magnetismus I. Teil: Elektrostatik und Elektrokinetik** von Prof. Dr. J. Classen in Hamburg. Geb. M. 5.—.

„ XLII: **Theorie der Elektrizität und des Magnetismus II. Tl.: Magnetismus u. Elektromagnetismus** von Prof. Dr. J. Classen in Hamburg. Geb. M. 7.—.

„ XLIII: **Theorie der ebenen algebraischen Kurven höherer Ordnung** von Dr. Heinr. Wieleitner in Speyer. Geb. M. 10.—.

„ XLIV: **Allgemeine Theorie der Raumkurven und Flächen II. Teil** von Prof. Dr. Victor Kommerell in Reutlingen und Professor Dr. Karl Kommerell in Heilbronn. Geb. M. 5.80.

„ XLV: **Niedere Analysis II. Teil: Funktionen, Potenzreihen, Gleichungen** von Prof. Dr. Hermann Schubert in Hamburg. Geb. M. 3.80.

„ XLVI: **Thetafunktionen u. hyperelliptische Funktionen** v. Oberlehrer E. Landfriedt i. Straßburg. Geb. M. 4.50.

„ XLVIII: **Thermodynamik II. Teil** von Prof. Dr. W. Voigt in Göttingen. Geb. M. 10.—.

„ XLIX: **Nichteuklidische Geometrie** von Prof. Dr. Heinr. Liebmann in Leipzig. Geb. M. 6.50.

„ L: **Gewöhnliche Differentialgleichungen beliebiger Ordnung** von Dr. J. Horn, Professor an der Bergakademie zu Clausthal. Geb. M. 10.—.

„ LI: **Liniengeometrie mit Anwendungen II. Teil** von Prof. Dr. Konrad Zindler i. Innsbruck. Geb. M. 8.—.

„ LII: **Theorie der geometrischen Konstruktionen** von Prof. Aug. Adler in Wien. Geb. M. 9.—.

Band LIII: **Grundlehren der neueren Zahlentheorie** von Prof. Dr. Paul Bachmann in Weimar. Geb. M. 6.50.

In Vorbereitung bzw. projektiert sind:

Darstellende Geometrie von Prof. Dr. Th. Schmid in Wien.
Geschichte der Mathematik von Prof. Dr. A. v. Braunmühl und Prof. Dr. S. Günther in München.
Dynamik von Prof. Dr. Karl Heun in Karlsruhe.
Technische Mechanik von Prof. Dr. Karl Heun in Karlsruhe.
Allgemeine Funktionentheorie von Dr. Paul Epstein in Straßburg.
Räumliche projektive Geometrie.
Geometrische Transformationen II. Teil von Prof. Dr. Karl Doehlemann in München.
Elliptische Funktionen von Dr. Karl Boehm in Heidelberg.
Allgemeine Formen- und Invariantentheorie von Prof. Dr. W. Franz Meyer in Königsberg.
Angewandte Potentialtheorie in elementarer Behandlung II. Teil von Prof. E. Grimsehl in Hamburg.
Liniengeometrie III. Teil von Prof. Dr. Konrad Zindler in Innsbruck.
Elektromagnetische Lichttheorie von Prof. Dr. J. Classen in Hamburg.
Gruppen- u. Substitutionentheorie v. Prof. Dr. E. Netto in Gießen.
Theorie der Flächen dritter Ordnung.
Mathematische Potentialtheorie v. Prof. Dr. A. Wangerin in Halle.
Elastizitäts- und Festigkeitslehre im Bauwesen von Dr. ing. H. Reißner in Berlin.
Elastizitäts- und Festigkeitslehre im Maschinenbau von Dr. Rudolf Wagner in Stettin.
Graphisches Rechnen von Prof. Aug. Adler in Wien.
Partielle Differentialgleichungen von Prof. J. Horn in Clausthal.
Vektorenanalyse.
Spezielle algebraische und transzendente ebene Kurven von Dr. Heinrich Wieleitner in Speyer.
Sphärische Astronomie von Dr. von Flotow in Charlottenburg.
Grundlehren der geographischen Ortsbestimmung von Dr. K. Graff in Hamburg.
Theorische Astronomie von Dr. Gust. Witt in Berlin.
Astrophysik.
Grundlagen der theoretischen Chemie von Dr. Franz Wenzel in Wien.
Analytische Geometrie auf der Kugel von Prof. Dr. Rich. Heger in Dresden.

Sammlung Schubert LIII

Grundlehren
der
Neueren Zahlentheorie

Von

Prof. Dr. Paul Bachmann

Mit 10 Figuren

Leipzig
G. J. Göschen'sche Verlagshandlung
1907

Spamersche Buchdruckerei in Leipzig.

Mit dem hiermit der Öffentlichkeit übergebenen Werke komme ich einer sehr liebenswürdigen Aufforderung der Verlagshandlung *G. J. Göschen* nach, ihr für die „Sammlung Schubert“ einen Band über Zahlentheorie zu liefern, „der das Thema in moderner Weise bis zu den quadratischen Formen einschließlich, ja bis zu den Zahlenkörpern“ behandeln, dabei aber der Tendenz dieser Sammlung entsprechend so geschrieben sein solle, daß das Buch von Jedem verstanden werden könne, der die Mathematik der höheren Schulen sich zu eigen gemacht hat. Nach Abfassung meiner anderen zahlentheoretischen Schriften konnte ich mich zur Übernahme einer solchen Aufgabe nur entschließen, indem ich das Schwergewicht eben in jenen Höhepunkt des zu behandelnden Gebietes verlegte, mich dabei jedoch auf den quadratischen Zahlenkörper beschränkend. Zu solcher Beschränkung nötigte mich schon allein der vorgesehene Umfang des Bandes zugleich mit der gedachten Tendenz, die gerade für die abstrakte zahlentheoretische Betrachtung eine gewisse Breite der Darstellung unerläßlich macht. Ich habe deshalb auch, um für die Theorie der quadratischen Formen und des quadratischen Körpers den erforderlichen Raum zu gewinnen, in bezug auf die Elemente der Zahlentheorie, die auch kaum einer „modernen“ Behandlung zugänglich gewesen wären, mich kürzer fassen und mit den notwendigsten und wichtigsten Betrachtungen begnügen müssen. Bei der Lehre von den quadratischen Formen habe ich dann versucht, die verschiedenen vorhandenen Auffassungen des Gegenstandes zu einem einheitlich geschlossenen Ganzen zu verknüpfen. Dies gelingt wesentlich mittels der Zahlengitter, durch welche einerseits eine anschauliche geometrische Deutung der Verhältnisse, andererseits in ihren Gitterzahlen die innere Verbindung zwischen den Formen und dem Körper und die eigentlichen Grundelemente für die Ideale des letz-

teren gewonnen werden. Durch solche ungezwungene Verkettung der verschiedenen Glieder dürfte nicht nur ein ästhetisch befriedigendes systematisches Gebilde, sondern auch tiefere Einsicht und Verständnis vom Wesen des Gegenstandes erzielt worden sein.

Die Tendenz meines Werkes, dem ich in Anbetracht der in ihm behandelten Zahlenkörper und -Gitter den Titel: Grundlehren (nicht: die Grundlehren) der neueren Zahlentheorie gegeben habe, ist ersichtlich die gleiche, wie diejenige der neuerdings im *Teubner*schen Verlage erschienenen Vorlesungen über Zahlentheorie von *J. Sommer*. Doch unterscheidet sich von diesem Werke das meinige nicht nur darin, daß es weniger hoch hinauf geht und, dem Charakter der Schubert-Sammlung gemäß mehr auf den Anfänger berechnet, den Elementen größere Berücksichtigung widmet, sondern auch in einem engeren Anschlusse an die Auffassungen *Dedekind*s bei der Theorie des quadratischen Körpers und vielleicht in einer noch flüssigeren Verschmelzung beider Theorien, derjenigen der Formen und des Körpers, in ein Ganzes. So hoffe ich, daß es neben dem des Herrn *Sommer* bestehen und ein Publikum finden werde, das sich durch dasselbe mühelos zu den reizvollen Gebieten zahlentheoretischer Forschung leiten und von der Art ihrer Ergebnisse unterrichten lassen will. —

Weimar, den 22. Juni 1907.

Inhaltsverzeichnis.

Erster Abschnitt.

Der rationale Zahlenkörper.

Erstes Kapitel.

Von der Teilbarkeit der ganzen Zahlen.

Zweites Kapitel.

Von der Kongruenz der Zahlen.

Drittes Kapitel.

Von den quadratischen Resten.

Viertes Kapitel.

Die Linearform $f = ax + by$.

Fünftes Kapitel.

Die quadratischen Formen.

Zweiter Abschnitt.

Der quadratische Zahlenkörper.

Erstes Kapitel.

Zahlen, Moduln, Ideale des Körpers.

Zweites Kapitel.

Die Einheiten des quadratischen Körpers.

Drittes Kapitel.

Die Teilbarkeit im quadratischen Körper.

Viertes Kapitel.

Ideale und Gitterzahlen.

Erster Abschnitt.

Der rationale Zahlenkörper.

Erstes Kapitel.

Von der Teilbarkeit der ganzen Zahlen.

1. Das Material, dessen Eigenschaften die Zahlentheorie zu entwickeln hat, bilden die sogenannten natürlichen Zahlen oder die positiven ganzen Zahlen 1, 2, 3, 4, 5, ..., allgemeiner die durch die Null und die negativen ganzen Zahlen erweiterte, nach beiden Richtungen unbegrenzte Zahlenreihe

(Z) $\quad \ldots, -4, -3, -2, -1, \quad 0, 1, 2, 3, 4, 5, \ldots$

Werden Zahlen dieser Reihe irgendwie durch Additionen, Subtraktionen oder Multiplikationen miteinander verknüpft, so erhält man bekanntlich stets wieder eine Zahl derselben Reihe. Dagegen führt die Division noch andere Zahlen, die gebrochenen herbei, welche zusammengenommen mit den ganzen die Gesamtheit der sogenannten rationalen Zahlen ausmachen. Nimmt man aber mit zwei Zahlen dieser letzteren Gesamtheit irgendeine der genannten vier Grundoperationen vor, so wird man stets wieder zu einer Zahl derselben Gesamtheit zurückgeführt, vorausgesetzt, was wir als selbstverständlich voraussetzen wollen, daß im Falle der Division der Divisor von Null verschieden sei. Man nennt nun ein System irgendwelcher Zahlen, welches die charakteristische, es gewissermaßen in sich abschließende Eigenschaft hat, daß, wenn eine beliebige seiner Zahlen mit einer beliebigen derselben durch eine der vier Grundoperationen verknüpft wird, die entstehende Zahl immer wieder jenem Systeme angehört, einen Zahlenkörper. Demnach ist die

Gesamtheit der rationalen Zahlen ein Körper, den wir den rationalen Zahlenkörper nennen und mit $\mathfrak{R}$ bezeichnen wollen. Unsere Betrachtungen bewegen sich bis auf weiteres ausschließlich im Gebiete dieses Körpers.

Wir nennen ferner Zahlenmodul eine Gesamtheit von Zahlen mit der engeren charakteristischen Eigenschaft, daß, wenn α sowohl wie β eine beliebige ihrer Zahlen bezeichnen, auch die Summe $\alpha + \beta$ und die Differenz $\alpha - \beta$ derselben Gesamtheit angehört. Die Zahlen (Z) teilen, wie schon bemerkt, diese Eigenschaft; demnach ist die Gesamtheit der rationalen ganzen Zahlen ein Zahlenmodul.

2. Es ist leicht, noch andere Zahlenmoduln anzugeben. Bezeichnen z. B. $a, b, c, \ldots$ eine Anzahl irgendwelcher Zahlen (die nicht rational zu sein brauchen), so bilden alle Zahlen von der Form

$$ax + by + cz + \ldots, \tag{1}$$

d. h. alle Zahlen, welche aus diesem Ausdrucke hervorgehen, wenn darin für $x, y, z, \ldots$ sämtliche ganze Zahlen gesetzt werden, offenbar einen Zahlenmodul. In der Tat, sind $\alpha, \beta, \gamma, \ldots$ und $\alpha', \beta', \gamma', \ldots$ ganzzahlige Werte der Unbestimmten $x, y, z, \ldots$, also

$$a\alpha + b\beta + c\gamma + \ldots, \qquad a\alpha' + b\beta' + c\gamma' + \ldots$$

zwei Zahlen der gedachten Gesamtheit, so bedeuten auch

$$\alpha + \alpha', \beta + \beta', \gamma + \gamma', \ldots \quad \text{und} \quad \alpha - \alpha', \beta - \beta', \gamma - \gamma', \ldots$$

ganzzahlige Wertsysteme, und folglich gehören auch die Summe

$$a(\alpha + \alpha') + b(\beta + \beta') + c(\gamma + \gamma') + \ldots$$

wie die Differenz

$$a(\alpha - \alpha') + b(\beta - \beta') + c(\gamma - \gamma') + \ldots$$

jener zwei Zahlen der gedachten Gesamtheit an. Wir bezeichnen diesen Zahlenmodul, also die Gesamtheit aller Zahlen von der Form (1), durch das Symbol

$$[a, b, c, \ldots]. \tag{2}$$

Man bemerke sogleich, daß man in einem solchen Symbole, ohne daß es seine Bedeutung verändert oder aufhört

dieselbe Gesamtheit von Zahlen zu bezeichnen, den Elementen $a, b, c, \ldots$ noch ein weiteres m hinzufügen, also

$$[a, b, c, \ldots] = [a, b, c, \ldots, m]$$

setzen kann, so oft dies letztere selbst eine Zahl des Moduls ist. Denn, ist etwa

$$m = a\alpha + b\beta + c\gamma + \ldots, \tag{3}$$

unter $\alpha, \beta, \gamma, \ldots$ ganze Zahlen verstanden, so ist

$$ax + by + cz + \ldots + mu = ax' + by' + cz' + \ldots,$$

wenn

$$x' = x + \alpha u, \quad y' = y + \beta u, \quad z' = z + \gamma u, \ldots$$

gesetzt wird; hiernach entspricht jedem Systeme ganzer Zahlen $x, y, z, \ldots, u$ ein System ganzer Zahlen $x', y', z', \ldots$, also ist die Gesamtheit der Zahlen von der Form

$$ax + by + cz + \ldots + mu$$

in derjenigen von der Form

$$ax' + by' + cz' + \ldots$$

enthalten; aber auch umgekehrt ist jede Zahl der letzteren Form eine solche der ersteren, da man sie aus ihr erhält, wenn $x = x', y = y', z = z', \ldots, u = 0$ gesetzt wird. Mithin bestehen in der Tat die Zahlenmoduln

$$[a, b, c, \ldots, u] \quad \text{und} \quad [a, b, c, \ldots]$$

aus denselben Zahlen. — Man wird daher in einem Modulsymbole $[a, b, c, \ldots, m]$, ohne daß es seine Bedeutung verändert, auch ein Element m unterdrücken können, falls dasselbe durch die übrigen Elemente in der Weise der Gleichung (3) ausdrückbar ist.

3. Ein einfaches Beispiel eines solchen Zahlenmoduls liefern die Vielfachen einer gegebenen ganzen Zahl m, nämlich die Zahlen der Reihe

$$\text{(M)} \quad \begin{cases} \ldots, -4m, -3m, -2m, -m, \\ 0, m, 2m, 3m, 4m, \ldots, \end{cases}$$

welche in unserer Bezeichnungsweise den eingliedrigen Zahlenmodul $[m]$ bilden, da sie aus dem Ausdrucke mu hervorgehen, wenn der Unbestimmten u alle ganzzahligen Werte

beigelegt werden. Ist nun n eine Zahl dieses Moduls, etwa $n = mq$, so wird m ein Teiler von n genannt, q heißt der Quotient $\frac{n}{m}$. Da man mit Vertauschung der Faktorenfolge auch $n = qm$ schreiben darf, so ist auch dieser Quotient ein Teiler von n und wird als solcher der zu m komplementäre Teiler von n genannt.

Wir dürfen uns auf die Betrachtung der positiven Teiler einer Zahl n beschränken, da offenbar ihre negativen aus ihnen erhalten werden, wenn man jene mit entgegengesetztem Vorzeichen nimmt; auch die Zahl n denken wir uns zunächst positiv.

Ist nun m ein Teiler von n, d. h. $n = q \cdot m$, und μ wieder ein Teiler von m, derart daß, unter γ eine ganze Zahl verstanden, $m = \gamma \cdot \mu$ gesetzt werden kann, so folgt $n = q\gamma \cdot \mu$, d. h. auch μ ist ein Teiler von n.

Statt dessen darf man auch sagen: Ist n ein Vielfaches von m (eine Zahl des Moduls $[m]$) und m ein Vielfaches von μ (eine Zahl des Moduls $[\mu]$), so ist n auch ein Vielfaches von μ (eine Zahl des Moduls $[\mu]$); oder auch so: Ist m eine Zahl des Moduls $[\mu]$, so ist der ganze Modul $[m]$ im Modul $[\mu]$ völlig enthalten.

Weil n sowohl gleich $1 \cdot n$ als auch gleich $n \cdot 1$ gesetzt werden kann, hat jede Zahl die Einheit und sich selbst zu Teilern. Hat sie außer diesen selbstverständlichen beiden Teilern keinen Teiler mehr, so wird sie unzerlegbar, andernfalls zerlegbar oder zusammengesetzt genannt.

Jeder Teiler von n ist aber offenbar gleich oder kleiner als n; da es nun nur eine endliche Menge ganzer Zahlen gibt, welche kleiner als n sind, so hat jede ganze Zahl n nur eine endliche Anzahl von verschiedenen Teilern und demnach, wenn sie zerlegbar ist, einen von 1 und von n verschiedenen kleinsten (positiven) Teiler, welcher p heiße, derart daß man $n = p \cdot n'$ setzen und unter n' eine positive ganze Zahl $< n$ verstehen darf.

Die Zahl p muß unzerlegbar sein, denn, hätte sie einen von 1 und p verschiedenen Teiler $\pi < p$, so daß $p = q \cdot \pi$ gesetzt werden könnte, so erhielte man $n = qn' \cdot \pi$, d. h. n hätte $\pi < p$ zum Teiler, gegen die Bedeutung von p. Ist nun auch die Zahl n' zerlegbar, so hat sie einen von 1 und n' verschiedenen kleinsten, also unzerlegbaren Teiler p', so

daß $n' = p'n''$ gesetzt und unter n'' eine ganze Zahl kleiner als n' verstanden werden darf, und man erhält $n = pp' \cdot n''$. Ist auch n'' noch zerlegbar, so kann man in gleicher Weise fortschließen, doch nicht ohne Ende, denn die Anzahl der abnehmenden ganzen Zahlen $n, n', n'', \ldots$ ist nur begrenzt. Mithin muß man in ihrer Reihe endlich zu einer nicht weiter zerlegbaren Zahl $n^{(\nu)}$ kommen, die deshalb $p^{(\nu)}$ heiße, und findet so die Zerlegung

(4) $$n = pp'p'' \ldots p^{(\nu)}$$

oder den **Satz:**

Jede (positive) ganze Zahl ist als ein Produkt aus einer endlichen Menge (positiver) unzerlegbarer Faktoren darstellbar, welche übrigens voneinander verschieden oder auch ganz oder teilweise einander gleich sein können. Wir werden diesem Satze bald eine wesentliche Verschärfung hinzuzufügen vermögen.

Beispiele:

1. $$60 = 2 \cdot 30 = 2 \cdot 2 \cdot 15 = 2 \cdot 2 \cdot 3 \cdot 5\,.$$

2. $$720 = 2 \cdot 360 = 2 \cdot 2 \cdot 180 = 2 \cdot 2 \cdot 2 \cdot 90 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 45$$
$$= 2 \cdot 2 \cdot 2 \cdot 2 \cdot 5 \cdot 9 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 5 \cdot 3 \cdot 3\,.$$

3. $$9249240 = 2 \cdot 2 \cdot 2 \cdot 5 \cdot 7 \cdot 7 \cdot 11 \cdot 11 \cdot 3 \cdot 13\,.$$

4. Nun seien a, b zwei gegebene (positive) ganze Zahlen. Sind sie beide Vielfache einer dritten ganzen Zahl m, so gilt dem vorigen zufolge dies auch von jedem Vielfachen ax von a und von jedem Vielfachen by von b. Da somit ax, by Zahlen des Moduls $[m]$ sind, so gehört der Definition eines solchen gemäß auch ihre Summe $ax + by$, welche ganzzahlige Werte x, y auch bedeuten, ihm an, d. h. der ganze Modul $[a, b]$ ist völlig enthalten im Modul $[m]$. Wird eine Zahl m, welche sowohl Teiler einer Zahl a, als auch Teiler einer Zahl b ist, ein gemeinsamer Teiler von a und b genannt, so läßt sich das Gefundene auch so aussprechen: jeder gemeinsame Teiler zweier ganzer Zahlen a, b ist auch Teiler einer jeden Zahl von der Form $ax + by$, wenn darin x, y ganze Zahlen bedeuten.

Dies vorausgeschickt sprechen wir nun einen Satz aus über die Beziehung jeder beliebigen Zahl zu einer gegebenen

Zahl m, der für alles Folgende geradezu als Grundsatz bezeichnet werden darf, nämlich den

Satz: Jede positive oder negative ganze Zahl n kann in die Form

$$n = q \cdot m + r \tag{5}$$

gesetzt werden, worin q, r ganze Zahlen, und zwar die letztere eine Zahl aus der Reihe $0, 1, 2, \ldots, m-1$ ist. In der Tat, entweder ist n ein Vielfaches von m, also von der Form (5), wenn $r = 0$ gedacht wird, oder n ist zwischen zwei aufeinanderfolgenden Vielfachen qm und $(q+1)m$ der Zahlenreihe (Z) enthalten, d. h. mit einer der Zahlen

$$qm+1, \quad qm+2, \quad qm+3, \ldots, \quad qm+m-1$$

identisch. Die Darstellung von n in der Form (5) ist zudem eindeutig bestimmt; wäre nämlich auch $n = q'm + r'$, wo r' ebenfalls eine Zahl der Reihe $0, 1, 2, \ldots, m-1$, so ergäbe sich $r' - r = (q - q') \cdot m$ als Vielfaches von m, während doch $r' - r$ absolut kleiner als m ist, demnach kann es nur Null, also $r' = r$ und daher dann auch $q' = q$ sein. Die nach diesem Grundsatze völlig bestimmte Zahl q heißt das größte in $\frac{n}{m}$ enthaltene Ganze: $q = E\left(\frac{n}{m}\right)$; r heißt der Rest, welchen die Zahl n in bezug auf m oder modulo m läßt.

Diesem Grundsatze zufolge wird man, wenn a, b zwei beliebig gegebene (positive) Zahlen bezeichnen, eine Gleichung ansetzen dürfen:

$$a = b\alpha + b_1, \tag{6}$$

wo $\alpha = E\left(\frac{a}{b}\right)$ und b_1 ganze Zahlen, die letztere aus der Reihe $0, 1, 2, \ldots, b-1$ also $< b$ ist. Gleicherweise darf man, wenn b_1 von Null verschieden,

$$b = b_1 \alpha_1 + b_2$$

setzen, wo $\alpha_1 = E\left(\frac{b}{b_1}\right)$ und b_2 ganze Zahlen, die letztere aus der Reihe $0, 1, 2, \ldots, b_1 - 1$, also $< b_1$ ist, und so wird man fortfahren können, doch nicht ohne Ende, denn

die Menge der abnehmenden positiven ganzen Zahlen b, b_1, b_2, ... ist nur begrenzt. Mithin muß man endlich zu einer der vorigen ähnlichen Gleichung kommen, in welcher aber der Rest Null ist, so daß der Prozeß damit endet. Man gewinnt also eine endliche Reihe von Gleichungen von der Form:

$$(7)\quad \begin{cases} a = b\alpha + b_1 \\ b = b_1\alpha_1 + b_2 \\ b_1 = b_2\alpha_2 + b_3 \\ \dots\dots\dots\dots \\ b_{\nu-2} = b_{\nu-1}\alpha_{\nu-1} + b_\nu \\ b_{\nu-1} = b_\nu\alpha_\nu , \end{cases}$$

die man als den, den Zahlen a, b entsprechenden *Euklid*ischen Algorithmus zu bezeichnen pflegt. Da nach der ersten dieser Gleichungen

$$b_1 = a \cdot 1 - b \cdot \alpha$$

ist, besteht infolge einer in Nr. 1 gemachten Bemerkung die Gleichheit der Moduln

$$[a, b] \quad \text{und} \quad [a, b, b_1],$$

und, weil nun $a = b \cdot \alpha + b_1 \cdot 1$ ist, auch die Gleichheit der Moduln

$$[a, b, b_1] \quad \text{und} \quad [b, b_1],$$

mithin findet sich

$$[a, b] = [b, b_1].$$

Mittels der ferneren Gleichungen des *Euklid*ischen Algorithmus (7) ergibt sich ebenso

$$[b, b_1] = [b_1, b_2], \quad [b_1, b_2] = [b_2, b_3], \dots$$

endlich auch $[b_{\nu-1}, b_\nu] = [b_\nu]$. Diese Gleichungen zusammenfassend erhalten wir als Resultat die Gleichung

$$(8)\qquad [a, b] = [b_\nu].$$

Ihr zufolge ist jede Zahl des Moduls $[a, b]$, insonderheit also auch a und b selber ein Vielfaches von b_ν, oder die durch den *Euklid*ischen Algorithmus (7) bestimmte Zahl b_ν und daher auch jeder Teiler von b_ν ist ein gemeinsamer Teiler von a, b. Andererseits wissen wir bereits, daß jeder gemeinsame Teiler von a, b auch Teiler jeder Zahl von der

Form $ax + by$, d. h. jeder Zahl des Moduls $[a, b]$ oder des ihm identischen Moduls $[b_\nu]$, insbesondere also auch Teiler von b_ν selbst ist. Hieraus folgt der

Satz: Die gemeinsamen Teiler von a, b sind identisch mit den sämtlichen Teilern der durch den Euklidischen Algorithmus (7) bestimmten Zahl b_ν, welche selbst solch ein Teiler und daher von ihnen allen der größte ist. Der genannte Algorithmus dient also dazu, den größten gemeinsamen Teiler der Zahlen a, b zu bestimmen.

Da endlich nach (8) b_ν eine Zahl des Moduls $[a, b]$, d. h. von der Form $ax + by$ ist, gibt es ganze Zahlen α, β derart, daß die Gleichung

$$(9) \qquad a\alpha + b\beta = b_\nu$$

stattfindet.

Beispiel: Für die Zahlen $a = 3378$, $b = 1059$ wird der *Euklid*ische Algorithmus:

$$\begin{aligned}
3378 &= 3 \cdot 1059 + 201 \\
1059 &= 5 \cdot 201 + 54 \\
201 &= 3 \cdot 54 + 39 \\
54 &= 1 \cdot 39 + 15 \\
39 &= 2 \cdot 15 + 9 \\
15 &= 1 \cdot 9 + 6 \\
9 &= 1 \cdot 6 + 3 \\
6 &= 2 \cdot 3 ;
\end{aligned}$$

mithin ist 3 größter gemeinsamer Teiler von 3378 und 1059. Um ihn in der Weise der Gleichung (9) mittels dieser Zahlen darzustellen, schreibe man vorstehende Gleichungen, von der vorletzten beginnend, folgendermaßen:

$$\begin{aligned}
3 &= 1 \cdot 9 - 1 \cdot 6 \\
6 &= 1 \cdot 15 - 1 \cdot 9 \\
9 &= 1 \cdot 39 - 2 \cdot 15 \\
15 &= 1 \cdot 54 - 1 \cdot 39 \\
39 &= 1 \cdot 201 - 3 \cdot 54 \\
54 &= 1 \cdot 1059 - 5 \cdot 201 \\
201 &= 1 \cdot 3378 - 3 \cdot 1059 ;
\end{aligned}$$

durch fortgesetzte Substitutionen in die erste dieser Gleichungen erhält man allmählich die Gleichungen:

$$3 = 2 \cdot 9 - 1 \cdot 15$$

$$3 = -5 \cdot 15 + 2 \cdot 39$$

$$3 = 7 \cdot 39 - 5 \cdot 54$$

$$3 = -26 \cdot 54 + 7 \cdot 201$$

$$3 = 137 \cdot 201 - 26 \cdot 1059$$

$$3 = 137 \cdot 3378 - 437 \cdot 1059\,,$$

deren letzte die gesuchte Gleichung ist.

5. Man nennt zwei Zahlen a, b, indem man von dem ihnen stets gemeinsamen Teiler 1 absieht, zwei Zahlen ohne gemeinsamen Teiler oder relativ prime oder teilerfremde Zahlen, wenn sie außer der Einheit keinen gemeinsamen Teiler haben. Dies wird offenbar dann und nur dann der Fall sein, wenn ihr durch den Euklidischen Algorithmus bestimmter größter gemeinsamer Teiler b_ν gleich 1 ist. Demnach besteht in diesem Falle für gewisse ganzzahlige Werte α, β die Gleichung

$$a\alpha + b\beta = 1\,, \tag{10}$$

oder die unbestimmte Gleichung

$$ax + by = 1 \tag{11}$$

ist in ganzen Zahlen x, y auflösbar. Die Auflösbarkeit dieser Gleichung in ganzen Zahlen x, y für den Fall teilerfremder a, b ist, wie sich zeigen wird, das folgenreichste Ergebnis, welches aus der fundamentalen in Gleichung (5) ausgesprochenen Tatsache der Zahlentheorie gezogen werden kann. Wir schließen daraus sofort den **Satz:**

Sind a, b zwei teilerfremde und c eine dritte ganze Zahl, so ist jeder gemeinsame Teiler von ac und b auch ein gemeinsamer Teiler von c und b. Denn, multipliziert man die Gleichung (10) mit c, so ist der gemeinsame Teiler von ac und b auch gemeinsamer Teiler ihrer Vielfachen $ac \cdot \alpha$ und $b \cdot \beta c$ und somit auch von deren Summe

$$ac \cdot \alpha + b \cdot \beta c = c\,.$$

Sind also auch c, b teilerfremd, so können ac und b nur die Einheit zu gemeinsamem Teiler haben, d. h. auch sie

sind teilerfremd, und wir schließen den Satz **(Euklidischer Fundamentalsatz):**

Sind zwei Zahlen a, c teilerfremd zu b, so ist auch ihr Produkt ac teilerfremd zu b. — Und hieraus folgt leicht allgemeiner: Sind $a, a', a'', \ldots$ und $b, b', b'' \ldots$ zwei Reihen von beliebig viel Zahlen, von denen jede Zahl der ersten Reihe relativ prim ist zu jeder Zahl der zweiten Reihe, so ist auch das Produkt $a\,a'\,a'' \ldots$ relativ prim zum Produkte $b\,b'\,b'' \ldots$ Denn dem vorstehenden Satze zufolge ist $a\,a'$, also auch $a\,a' \cdot a''$, usw., endlich das Produkt $a\,a'\,a'' \ldots$ zu jeder der Zahlen $b, b', b'', \ldots$ oder jede dieser Zahlen zu jenem Produkte teilerfremd, demnach ist auch $b\,b'$, also auch $b\,b' \cdot b''$, usw., endlich das Produkt $b\,b'\,b'' \ldots$ teilerfremd zu $a\,a'\,a'' \ldots$, w. z. b. w. Nimmt man die ersteren Zahlen alle gleich a, die letzteren alle gleich b an und nennt h und k ihre Anzahl resp., so schließt man insbesondere, daß für teilerfremde a, b auch beliebige positive ganze Potenzen a^h, b^k teilerfremd sind.

Man nennt nun eine positive ganze Zahl p eine Primzahl, wenn sie die Eigenschaft hat, daß jedes Produkt ganzer Zahlen nur dann durch p teilbar ist, wenn wenigstens einer dieser seiner Faktoren es ist. Demnach ist jede Primzahl eine unzerlegbare Zahl, denn, wäre $p = a \cdot b$ eine Zerlegung von p in zwei von 1 und p verschiedene Faktoren, so wäre das Produkt $a \cdot b$ und doch keiner der Faktoren, da sie kleiner sind als p, durch p teilbar, mithin könnte p keine Primzahl sein. Aber jede unzerlegbare Zahl n ist auch Primzahl; denn sonst gäbe es ein durch n teilbares Produkt von Faktoren, deren keiner durch n teilbar ist und folglich, da n nur die beiden Teiler 1 und n hat, mit n nur den Teiler 1 gemeinsam haben kann; jeder dieser Faktoren wäre also teilerfremd mit n und daher wäre dies auch ihr Produkt, welches doch im Gegenteil durch n teilbar vorausgesetzt ist. Man sieht aus diesen beiden Momenten, daß Primzahlen und unzerlegbare positive ganze Zahlen ein und dasselbe sind.

Nun hatten wir für jede positive ganze Zahl n eine Zerlegung in unzerlegbare positive Zahlen nachgewiesen von der Form (4); die Faktoren derselben dürfen daher jetzt auch als Primfaktoren bezeichnet werden. Gäbe es nun noch eine zweite Zerlegung von n in Primfaktoren, etwa durch die Gleichung

$$n = q\,q'\,q'' \ldots q^{(\mu)},$$

so erhielte man die Gleichheit

$$(12)\qquad p p' p'' \dots p^{(\nu)} = q q' \dots q^{(\mu)}$$

zweier Zahlen, deren rechtsstehende infolge derselben durch den Primfaktor p der linksstehenden teilbar wäre. Daher müßte einer der Faktoren rechts, etwa die Primzahl q den Teiler p haben, und da q als unzerlegbare Zahl nur die Teiler 1 und q besitzt, deren erster von p verschieden ist, müßte q mit dem Teiler p identisch, $q = p$ sein. Somit höbe sich aus (12) rechts und links der Faktor p und q fort und man erhielte die Gleichung

$$p' p'' \dots p^{(\nu)} = q' \dots q^{(\mu)},$$

die nun ähnliche Schlüsse verstattet. Solange auf der einen oder der andern Seite noch ein Primfaktor sich findet, muß auch die andere Seite durch ihn teilbar sein, was seine Identität mit einem Primfaktor der anderen Seite ergibt, und somit erkennt man, daß nicht nur beiderseits gleich viel, sondern auch genau dieselben Primfaktoren befindlich, daher die beiden Zerlegungen der Zahl n miteinander identisch sein müssen. Man findet folglich den nachstehenden Satz, welcher den Satz (4) wesentlich vervollständigt, und als Fundamentalsatz von der Teilbarkeit ganzer Zahlen bezeichnet werden soll:

Jede positive ganze Zahl n kann auf eine eindeutig bestimmte Weise als ein Produkt aus einer endlichen Anzahl von Primfaktoren dargestellt werden. — Indem man die etwa untereinander gleichen dieser Primfaktoren immer in eine Potenz zusammenfaßt, nimmt solche Darstellung die Form an:

$$(13)\qquad n = p^{\alpha} \cdot p'^{\alpha'} \cdot p''^{\alpha''} \dots,$$

worin $p, p', p'', \dots$ verschiedene Primzahlen, $\alpha, \alpha', \alpha'', \dots$ positive ganze Exponenten bedeuten.

Beispiele:

$$60 = 2^2 \cdot 3^1 \cdot 5^1, \qquad 720 = 2^4 \cdot 3^2 \cdot 5^1,$$

$$9249240 = 2^3 \cdot 5^1 \cdot 7^2 \cdot 11^2 \cdot 3^1 \cdot 13^1, \qquad 4704 = 2^5 \cdot 3^1 \cdot 7^2,$$

$$6534 = 2^1 \cdot 3^3 \cdot 11^2.$$

6. Ist d der größte gemeinsame Teiler zweier Zahlen a, b und

$$(14)\qquad a = d a', \quad b = d b',$$

so müssen a', b' teilerfremd sein; denn, hätten sie einen von 1 verschiedenen gemeinsamen Teiler δ, so daß $a' = \delta\alpha$, $b' = \delta\beta$ gesetzt werden könnte, unter α, β ganze Zahlen verstanden, so ergäbe sich

$$a = d\delta \cdot \alpha, \quad b = d\delta \cdot \beta$$

und a, b hätten den gemeinsamen Teiler $d\delta > d$. Umgekehrt wird d der größte gemeinsame Teiler von a, b sein, wenn die Formeln (14) statthaben und a', b' darin teilerfremd sind. Denn, ist δ der größte gemeinsame Teiler von a, b, so muß d als gemeinsamer Teiler dieser Zahlen ein Teiler von δ oder δ ein Vielfaches von d, $\delta = dd'$ sein; da aber $a = da'$, $b = db'$ durch $\delta = dd'$, d. h. die teilerfremden Zahlen a', b' durch d' teilbar sein sollen, muß $d' = 1$, d. h. $\delta = d$ sein, w. z. b. w.

Man nennt eine Zahl, welche sowohl durch a als durch b teilbar, d. h. ein Vielfaches jeder der beiden Zahlen a, b ist, ein gemeinsames Vielfaches von a, b. Soll ein Vielfaches von a,

$$m = az,$$

auch Vielfaches von b, d. h. durch b teilbar sein, so muß den Gleichungen (14) gemäß $da'z$ durch db' oder $a'z$ durch b' teilbar sein, was erfordert, daß z durch b' teilbar sei, da a', b' teilerfremd sind. Man setze demgemäß $z = b'y$, wo y ganzzahlig gedacht wird; dadurch erhält jedes gemeinsame Vielfache von a, b die Gestalt

$$m = ab'y = \frac{ab}{d} \cdot y.$$

Jede Zahl dieser Gestalt ist aber auch wirklich ein gemeinsames Vielfaches von a, b, da man schreiben kann

$$\frac{ab}{d} \cdot y = a \cdot b'y = b \cdot a'y,$$

und unter allen Zahlen dieser Gestalt ist ersichtlich die Zahl $\frac{ab}{d}$ die kleinste. Man gewinnt so folgenden

Satz: Die gemeinsamen Vielfachen zweier Zahlen a, b sind identisch mit den sämtlichen Vielfachen ihres kleinsten gemeinsamen Vielfachen, welches man erhält, wenn man ihr Produkt durch ihren größten gemeinsamen Teiler dividiert.

Das kleinste gemeinsame Vielfache zweier teilerfremden Zahlen a, b ist sonach ihr Produkt ab, denn in diesem Falle ist $d = 1$.

Man kann diese Betrachtungen verallgemeinern. Sind

$$(15) \qquad a, b, c, \ldots$$

beliebig viel ganze Zahlen, so haben sie, da jede von ihnen nur eine endliche Anzahl von Teilern hat, auch nur eine endliche Anzahl gemeinsamer Teiler und somit auch einen größten gemeinsamen Teiler. Die sämtlichen gemeinsamen Teiler der Zahlen (15) sind identisch mit den Teilern dieses ihres größten gemeinsamen Teilers. Man beweist dies durch allgemeine Induktion: der Satz steht schon fest für zwei Zahlen; wir nehmen an, er gelte sogar bereits für die Zahlen $b, c, \ldots$, und folgern ihn für die um eins größere Anzahl der Zahlen (15), und damit seine allgemeine Gültigkeit. Nach der Annahme ist, wenn δ den größten gemeinsamen Teiler der Zahlen $b, c, \ldots$ bedeutet, jeder ihnen gemeinsame Teiler auch Teiler von δ. Daher muß jeder gemeinsame Teiler aller Zahlen (15) als gemeinsamer Teiler auch der Zahlen $b, c, \ldots$ ein Teiler von δ, also gemeinsamer Teiler von a und δ, also auch ein Teiler des größten gemeinsamen Teilers d von a und δ sein. Dieser letztere d aber ist, weil er zugleich mit δ auch gemeinsamer Teiler von $b, c, \ldots$ ist, ersichtlich selbst ein allen Zahlen (15) gemeinsamer Teiler und von ihnen allen der größte, da d durch jeden andern von ihnen aufgeht; und weil auch jeder seiner Teiler allen Zahlen (15) gemeinsam sein muß, so stimmen seine Teiler und die den Zahlen (15) gemeinsamen Teiler in der Tat überein.

Ist d der größte gemeinsame Teiler der Zahlen (15) und

$$(16) \qquad a = da', \quad b = db', \quad c = dc', \ldots,$$

so sind $a', b', c', \ldots$ Zahlen ohne einen (von Eins verschiedenen) gemeinsamen Teiler; denn, hätten sie einen solchen δ, so daß man setzen könnte

$$a' = \delta\alpha, \quad b' = \delta\beta, \quad c' = \delta\gamma, \ldots,$$

so ergäbe sich

$$a = d\delta \cdot \alpha, \quad b = d\delta \cdot \beta, \quad c = d\delta \cdot \gamma, \ldots$$

und die Zahlen (15) hätten den Teiler $d\delta > d$ gemeinsam, gegen die Bedeutung von d. Umgekehrt wird d größter gemeinsamer Teiler der Zahlen (15) sein, wenn die Gleichungen (16) stattfinden, während $a', b', c', \ldots$ ohne gemeinsamen Teiler sind; denn wäre δ der größte gemeinsame Teiler von $a, b, c, \ldots$, so müßte d, weil den Gleichungen (16) zufolge ein gemeinsamer Teiler der Zahlen $a, b, c, \ldots$, ein Teiler von δ oder δ ein Vielfaches von d, $\delta = dd'$ sein und da die Zahlen (16) durch δ teilbar wären, fände sich d' als ein gemeinsamer Teiler von $a', b', c', \ldots$ also gleich 1 und somit $\delta = d$.

Eine Zahl m, welche Vielfaches von jeder der Zahlen (15) ist, heißt ein gemeinsames Vielfaches derselben. Das kleinste derselben hat die Eigenschaft, daß seine Vielfachen mit den sämtlichen gemeinsamen Vielfachen der Zahlen (15) identisch sind. Dieser Satz steht schon fest für zwei Zahlen; nehmen wir an, er gelte auch bereits für die Zahlen $b, c, \ldots$, so daß, wenn μ deren kleinstes gemeinsames Vielfache bedeutet, jedes gemeinsame Vielfache derselben ein Vielfaches von μ ist. Daher muß dann jedes gemeinsame Vielfache aller Zahlen (15), da es auch ein solches der Zahlen $b, c, \ldots$ ist, ein Vielfaches von μ, demnach ein gemeinsames Vielfaches von a und μ und somit auch ein Vielfaches von deren kleinstem gemeinsamen Vielfachen m sein. Dies letztere m aber ist, weil zugleich mit μ auch ein gemeinsames Vielfaches von $b, c, \ldots$, selbst ein gemeinsames Vielfaches aller Zahlen (15) und von diesen ihnen gemeinsamen Vielfachen das kleinste, da es in jedem andern von ihnen aufgeht; auch wird jedes seiner Vielfachen mit m zugleich ein gemeinsames Vielfaches aller Zahlen (15) sein. Demnach stimmen seine Vielfachen mit den sämtlichen gemeinsamen Vielfachen der Zahlen (15) überein. Hierdurch ist die Allgemeingültigkeit des behaupteten Satzes erwiesen.

Das kleinste gemeinsame Vielfache mehrerer Zahlen $a, b, c, \ldots$, die zu je zweien teilerfremd sind, ist gleich ihrem Produkte. Dieser Satz ist schon festgestellt für zwei solche Zahlen; nehmen wir an, er gelte auch schon für die Zahlen $b, c, \ldots$, so ist deren kleinstes gemeinsame Vielfache μ gleich $bc \ldots$ Dem zuvor Bewiesenen zufolge ist aber das kleinste gemeinsame Vielfache m aller Zahlen (15) gleich demjenigen der Zahlen a und μ, und folglich, da a

nach der Voraussetzung zu jeder der Zahlen $b, c, \ldots$ also auch zu ihrem Produkte μ teilerfremd ist, gleich dem Produkte $a\mu = abc \ldots$

Zweites Kapitel.

Von der Kongruenz der Zahlen.

1. Nach der Grundtatsache der Zahlentheorie läßt jede positive oder negative ganze Zahl, durch eine gegebene ganze Zahl m geteilt, einen bestimmten Rest aus der Reihe der Zahlen $0, 1, 2, \ldots, m-1$. Sind n, n' zwei ganze Zahlen und

$$(1) \qquad n = qm + r, \quad n' = q'm + r', \quad (0 \gtreqless r \gtreqless m-1, \quad 0 \gtreqless r' \gtreqless m-1),$$

so heißen n, n' nach m oder modulo m gleichrestig oder kongruent, wenn die Reste r, r' einander gleich, sie heißen inkongruent nach m, wenn r, r' voneinander verschieden sind. Da im ersteren Falle die Differenz

$$n - n' = (q - q') \cdot m$$

durch m teilbar oder eine Zahl des Moduls $[m]$ ist, im anderen Falle aber diese Differenz

$$n - n' = (q - q') \cdot m + r - r'$$

nicht durch m teilbar ist, da dann $r - r'$ eine von Null verschiedene Zahl der Reihe $-(m-1), -(m-2) \ldots, (m-2), (m-1)$ ist, dürfen wir auch sagen: die Zahlen n, n' sind nach m kongruent oder inkongruent, je nachdem ihre Differenz $n - n'$ dem Modul $[m]$ angehört oder nicht. Im ersteren Falle setzen wir nach *Gauss*

$$(2) \qquad n \equiv n' \pmod{m}$$

und nennen eine Beziehung dieser Art eine Kongruenz.

Hier gelten folgende einfache Grundregeln:

1. Sind zwei Zahlen n', n'' einer dritten Zahl n (mod. m) kongruent, so sind sie es auch untereinander. Denn die vorausgesetzten Kongruenzen

$$n \equiv n', \quad n \equiv n'' \pmod{m}$$

besagen, daß die Differenzen $n-n'$, $n-n''$ Zahlen des Moduls $[m]$ sind, demnach gehört auch ihre Differenz

$$(n-n'')-(n-n')=n'-n''$$

diesem Modul an und somit ist $n' \equiv n''$ (mod. m).

2. Aus zwei Kongruenzen

(3) $$n \equiv n', \quad N \equiv N' \quad (\text{mod.}\, m)$$

erschließt man auch die durch Addition, Subtraktion und Multiplikation derselben hervorgehenden Kongruenzen

(4) $$\left.\begin{cases} n+N \equiv n'+N' \\ n-N \equiv n'-N' \\ nN \equiv n'N' \end{cases}\right\} \quad (\text{mod.}\, m).$$

Denn nach (3) sind die Differenzen $n-n'$, $N-N'$ Zahlen des Moduls $[m]$; daher ist auch sowohl ihre Summe als auch ihre Differenz, d. h. sowohl

$$n+N-(n'+N') \quad \text{als auch} \quad (n-N)-(n'-N')$$

eine Zahl desselben Moduls, was die beiden ersten der Kongruenzen (4) aussagen. Aber auch die Vielfachen $(n-n')\cdot N$ und $(N-N')\cdot n'$ der in $[m]$ enthaltenen Zahlen $n-n'$, $N-N'$ gehören (vor. Kap. Nr. 2, 3) dem Modul $[m]$ an, somit ist auch ihre Summe

$$(n-n')\,N+(N-N')\,n'=n\,N-N'\cdot n'$$

eine Zahl des Moduls $[m]$, wie die dritte der Kongruenzen (4) behauptet.

3. Aus der Kongruenz

(5) $$nN \equiv n'N \quad (\text{mod.}\, m)$$

folgt diese andere:

(6) $$n \equiv n' \quad \left(\text{mod.}\, \frac{m}{d}\right),$$

wenn d den größten gemeinsamen Teiler von m und N bedeutet. Denn nach (5) ist die Differenz $(n-n')\,N$ teilbar durch m; setzt man nun $m=d\,m'$, $N=d\,N'$, so daß m', N' teilerfremd sind, so muß, da $(n-n')\,N'$ teilbar ist durch m', der Faktor $n-n'$ durch $m'=\frac{m}{d}$ teilbar sein, wie die Kongruenz (6) aussagt.

Hiernach darf in einer Kongruenz ein etwa vorhandener gemeinsamer Faktor beider Seiten nur dann unterdrückt werden, wenn er zum Modul teilerfremd ist, denn aus (5) ergibt sich nur dann notwendig $n \equiv n' \pmod{m}$, wenn $d = 1$ ist.

4. Aus der Kongruenz

$$n \equiv n' \pmod{m} \tag{7}$$

folgt auch für jeden Teiler d von m die Kongruenz

$$n \equiv n' \pmod{d}; \tag{8}$$

denn, ist die Differenz $n - n'$ eine Zahl des Moduls $[m]$, so ist sie, da dieser (Kap. 1 Nr. 2) völlig im Modul $[d]$ enthalten ist, auch eine Zahl dieses letzteren Moduls und die Kongruenz (8) erfüllt.

5. Besteht die Kongruenz zweier Zahlen n, n' nach verschiedenen Moduln $a, b, c, \ldots$, so besteht sie auch nach deren kleinstem gemeinsamen Vielfachen m. Denn die Differenz $n - n'$ muß, wenn sie ein Vielfaches jeder der Zahlen $a, b, c, \ldots$ ist, zugleich auch ein solches von m sein. — Sind insbesondere die Moduln $a, b, c, \ldots$ zu je zweien teilerfremd, so folgt aus der Kongruenz zweier Zahlen n, n' nach allen jenen Moduln ihre Kongruenz auch nach deren Produkt, denn jetzt ist (Kap. 1, Schluß) das kleinste gemeinsame Vielfache m der Moduln gleich diesem Produkte.

2. Nach diesen Regeln ergibt sich ein wichtiger Satz. Sei nämlich

$$f(x) = a_k x^k + a_{k-1} x^{k-1} + \ldots + a_1 x + a_0 \tag{9}$$

eine ganze Funktion der Unbestimmten x mit ganzzahligen Koeffizienten $a_k, a_{k-1}, \ldots, a_0$; für jeden ganzzahligen Wert der Unbestimmten nimmt sie gleichfalls einen ganzzahligen Wert an. Wenn nun α, β zwei nach m kongruente Zahlen bedeuten, so folgt aus der wiederholten Multiplikation der Kongruenz

$$\beta \equiv \alpha \pmod{m} \tag{10}$$

mit sich selbst für jeden ganzzahligen Exponenten i die Kongruenz

$$\beta^i \equiv \alpha^i \pmod{m},$$

und, wenn diese mit der selbstverständlichen anderen: $a_i \equiv a_i \pmod{m}$ multipliziert wird, auch

(11) $$a_i \beta^i \equiv a_i \alpha^i \pmod{m};$$

die Addition endlich der den Werten $i = k, k-1, \ldots 2, 1, 0$ entsprechenden Kongruenzen (11) ergibt offenbar die folgende:

(12) $$f(\beta) \equiv f(\alpha) \pmod{m}$$

und somit den **Satz:**

Die Werte, welche eine ganze Funktion von x mit ganzzahligen Koeffizienten für zwei einander kongruente Werte der Unbestimmten x annimmt, sind selbst kongruent.

Schreibt man z. B. die Zahl 9523 in der gewöhnlichen dekadischen Form

$$9523 = 9 \cdot 10^3 + 5 \cdot 10^2 + 2 \cdot 10^1 + 3 = f(10)$$

und beachtet, daß $10 \equiv 1 \pmod{9}$ ist, so ergibt sich

$$f(10) \equiv f(1)$$

oder

$$9523 \equiv 9 + 5 + 2 + 3 \pmod{9},$$

d. h. der bekannte Satz: Eine Zahl gibt durch 9 geteilt denselben Rest, wie die Quersumme ihrer Ziffern.

Um die inkongruenten Werte der Funktion $f(x)$ zu erhalten, braucht man jenem Satze zufolge x nur alle Reste $0, 1, 2, \ldots, m-1 \pmod{m}$ durchlaufen zu lassen. Es ist nicht gesagt, daß die Funktion $f(x)$ dann auch selbst alle Reste, z. B. den Rest Null (mod. m) ergeben wird, im Gegenteil entsteht hier eine Aufgabe, welche das Analogon zur Auflösung der Gleichung

(13) $$f(x) = 0$$

oder zur Bestimmung der sogenannten Wurzeln dieser Gleichung ausmacht, nämlich die Aufgabe:

Bei gegebener Funktion $f(x)$ diejenigen etwa vorhandenen ganzzahligen Werte x zu ermitteln, für welche die Kongruenz

(14) $$f(x) \equiv 0 \pmod{m}$$

erfüllt, nämlich $f(x)$ durch m teilbar wird. Während eine Gleichung (13) stets nur eine endliche Menge von Lösungen

oder Wurzeln hat, ist die Anzahl der Lösungen einer Kongruenz (14), wenn es deren überhaupt eine gibt, stets unendlich groß, da, wenn $f(\alpha) \equiv 0$ ist, für jede der unendlich vielen mit α kongruenten Zahlen $\beta = \alpha + m \cdot z$ ebenfalls $f(\beta) \equiv 0$ ist, wie zuvor festgestellt worden. Man betrachtet indessen sämtliche untereinander kongruente Lösungen stets nur als eine einzige Wurzel der Kongruenz, und bei dieser Auffassung hat auch jede Kongruenz nur eine endliche Anzahl von Wurzeln.

Ist insbesondere der Modul m eine Primzahl p, so gilt sogar der gleiche Satz, wie von den Gleichungen, daß nämlich die Anzahl der Wurzeln einer Kongruenz (mod. p) nicht größer sein kann als ihr Grad. Dabei bedarf es aber einer Definition für den sogenannten Grad einer Kongruenz. Da offenbar die beiden ganzen Funktionen

$$a_{k-1} x^{k-1} + \ldots + a_1 x + a_0$$

$$a_k x^k + a_{k-1} x^{k-1} + \ldots + a_1 x + a_0 ,$$

falls a_k teilbar ist durch p, für jeden ganzzahligen Wert von x einander kongruent sind (mod. p), müssen auch ihre Wurzeln identisch sein, d. h. diejenigen Werte von x, für welche die eine teilbar wird durch p, müssen auch die andere durch p teilbar machen; man darf daher, ohne daß sich die Wurzeln der Kongruenz

$$(15) \qquad a_k x^k + a_{k-1} x^{k-1} + \ldots + a_1 x + a_0 \equiv 0 \pmod{p}$$

ändern, das durch p teilbare erste Glied, sowie auch jedes weitere, welches etwa durch p teilbar wäre, weglassen. Daher heißt eine solche Kongruenz dann und nur dann vom Grade k, wenn das höchste Glied, dessen Koeffizient durch p nicht teilbar ist, den Exponenten k hat. Wären sämtliche Koeffizienten der Kongruenz (15) teilbar durch p, so besäße diese Kongruenz überhaupt keinen Grad und wäre identisch, nämlich für jedes ganzzahlige x erfüllt.

Der oben ausgesprochene Satz beweist sich nun durch allgemeine Induktion. Betrachten wir zuvörderst die allgemeine Kongruenz vom Grade 1, nämlich

$$(16) \qquad a_1 x + a_0 \equiv 0 \pmod{p},$$

wo also a_1 nicht durch p teilbar ist. Sie kann nie mehr

als eine Wurzel haben, denn, sind $x = \alpha$ und $x = \beta$ zwei Lösungen derart, daß

$$a_1 \alpha + a_0 \equiv 0 , \qquad a_1 \beta + a_0 \equiv 0$$

wäre, so ergibt sich durch Subtraktion dieser beiden Kongruenzen

$$a_1(\alpha - \beta) \equiv 0 \pmod{p} ,$$

und, da a_1 nicht teilbar ist durch p, muß es $\alpha - \beta$, d. h. $\alpha \equiv \beta \pmod{p}$ sein; alle etwaigen Lösungen von (16) bilden demnach nur eine Wurzel. — Nachdem dies festgestellt ist, nehmen wir den zu beweisenden Satz auch schon für alle Kongruenzen kleineren als des $k$ten Grades als bewiesen an und zeigen, daß er dann auch für die Kongruenz (15) vom Grade k gilt. Hätte diese aber im Gegenteil mehr als k Wurzeln, mindestens also $k+1$ inkongruente Lösungen $\alpha, \alpha_1, \alpha_2, \ldots, \alpha_k$, so wäre die Differenz der beiden Ausdrücke

$$a_k x^k + a_{k-1} x^{k-1} + \ldots + a_1 x + a_0 ,$$

$$a_k(x - \alpha_1)(x - \alpha_2) \ldots (x - \alpha_k)$$

eine ganze, ganzzahlige Funktion von x, deren Grad (mod. p) höchstens $k-1$ ist, da die Potenz x^k in der Differenz sich hebt; die Kongruenz

$$(a_k x^k + a_{k-1} x^{k-1} + \ldots + a_0) - a_k(x-\alpha_1)\ldots(x-\alpha_k) \equiv 0 \pmod{p}$$

hätte aber k Wurzeln $\alpha_1, \alpha_2, \ldots, \alpha_k$, da sowohl der Minuendus als der Subtrahendus für jeden dieser Werte von x durch p teilbar wird, und daher müßte die Kongruenz nach der gemachten Annahme identisch, mithin auch für den Wert $x = \alpha$ erfüllt sein. Da aber für diesen Wert der Minuendus nach Voraussetzung kongruent Null ist, erhielte man die Kongruenz

$$a_k(\alpha - \alpha_1)(\alpha - \alpha_2) \ldots (\alpha - \alpha_k) \equiv 0 \pmod{p} ,$$

die nicht stattfinden kann, denn weder kann der höchste Koeffizient a_k der Kongruenz (15) noch eine der Differenzen $\alpha - \alpha_1, \alpha - \alpha_2, \ldots, \alpha - \alpha_k$, da α als mit den Zahlen $\alpha_1, \alpha_2, \ldots, \alpha_k$ inkongruent gedacht ist, durch p teilbar sein, und somit kann es auch das Produkt selbst nicht sein. Dieser Widerspruch erweist die Richtigkeit des Satzes auch für die Kongruenz (15) des Grades k und somit seine Allgemeingültigkeit.

3. Indem wir nun wieder den Modul m als beliebig gegeben denken, wollen wir alle untereinander (mod. m) kongruenten Zahlen in eine Klasse zusammenfassen, die wir dann eine Restklasse (mod. m) nennen. Da die Zahlen $0, 1, 2, \ldots, m-1$ zu je zweien inkongruent, also verschiedenen Restklassen zugehörig sind, jede andere Zahl n aber einer von jenen kongruent, also in deren Restklasse befindlich ist, so gibt es m verschiedene Restklassen, die wir unzweideutig repräsentieren können, wenn wir aus jeder von ihnen nach Belieben ein Individuum

$$r_0, r_1, r_2, \ldots, r_{m-1} \tag{17}$$

herausgreifen. Denn, ist i der Rest, welchen r_i (mod. m) läßt, so gehört r_i der dem Reste i entsprechenden Klasse an und die durch r_i repräsentierte Restklasse ist die Gesamtheit aller Zahlen mit dem Reste i (mod. m). Ein solches System repräsentierender Zahlen (17) nennen wir kurz ein vollständiges Restsystem oder ein System inkongruenter Zahlen (mod. m). Das einfachste ist das System der Zahlen

$$0, 1, 2, \ldots, m-1, \tag{18}$$

welches das System der kleinsten positiven Reste heißt. Für den Fall eines ungeraden Moduls m heben wir ein anderes wegen seiner Wichtigkeit für die Folge hervor, das System der absolut kleinsten Reste:

$$\begin{cases} -\frac{m-1}{2}, \; -\frac{m-3}{2}, \ldots, \; -2, \; -1, \; 0, 1, 2, \ldots, \\ \qquad\qquad\qquad \frac{m-3}{2}, \; \frac{m-1}{2}, \end{cases} \tag{19}$$

dessen m Zahlen in der Tat zu je zweien inkongruent sind, da deren Differenz absolut kleiner als m und von Null verschieden und daher durch m nicht teilbar ist.

Z. B. ist für $m = 17$ das System der kleinsten positiven Reste:

$$0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16,$$

dasjenige der absolut kleinsten Reste:

$$-8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8;$$

aber auch das System der Zahlen:

$$34,\ -16,\ 19,\ 37,\ 4,\ -12,\ -45,\ 24,\ 8,\ -8,\ 27,\ 11,\ 46,\ -4,\ 14,\ -19,\ -1$$

stellt ein vollständiges Restsystem dar, da sie den Zahlen des erstbezeichneten Systems der Reihe nach kongruent sind.

Nun haben ersichtlich alle Zahlen einer Klasse (mod. m) den gleichen größten Teiler mit dem Modul gemeinsam. Denn, ist $n \equiv n'$ (mod. m), d. h. $n = n' + mz$, so geht jeder den Zahlen n', m gemeinsame Teiler auch in n, und jeder den Zahlen n, m gemeinsame Teiler wegen $n' = n - mz$ auch in n' auf. Ist daher eine Zahl einer Restklasse relativ prim zum Modul, so sind sie es sämtlich, und daher verteilen sich alle zu m teilerfremden Zahlen in diejenigen Restklassen und erfüllen auch diese, deren Repräsentanten zu m teilerfremd sind. Zieht man diese aus dem vollständigen Restsysteme heraus und nennt sie

$$\varrho_1,\ \varrho_2,\ \varrho_3,\ \ldots,\ \varrho_\mu, \tag{20}$$

so repräsentiert dies sogenannte reduzierte Restsystem (mod. m) sämtliche zu m teilerfremde Zahlen in Restklassen (mod. m) verteilt. Die Anzahl μ dieser Klassen, d. i. die Anzahl der Zahlen $0, 1, 2, \ldots, m-1$, welche teilerfremd sind zu m, wird als eine von m abhängige Zahl gewöhnlich durch das Funktionszeichen

$$\mu = \varphi(m) \tag{21}$$

bezeichnet.

4. Man denke die Zahl m irgendwie in Faktoren $a, b, c, \ldots$ zerlegt, die zu zweien teilerfremd sind, z. B. in die verschiedenen Primzahlpotenzen, aus denen sie nach Kap. 1 zusammengesetzt ist. Dann wird jede Zahl n der Reihe (18) durch $a, b, c, \ldots$ geteilt bzw. einen der Reste

$$\begin{cases} 0, 1, 2, \ldots, a-1 & (\text{mod. } a) \\ 0, 1, 2, \ldots, b-1 & (\text{mod. } b) \\ 0, 1, 2, \ldots, c-1 & (\text{mod. } c) \\ \ldots\ldots\ldots\ldots \end{cases} \tag{22}$$

und folglich eine bestimmte Kombination aus je einem Elemente dieser verschiedenen Restsysteme ergeben. Zwei ver-

schiedene Zahlen n, n' jener Reihe geben aber auch verschiedene Restkombinationen. Denn, wäre zugleich

$$n \equiv \alpha \pmod{a}, \quad n \equiv \beta \pmod{b}, \quad n \equiv \gamma \pmod{c}, \ldots$$
$$n' \equiv \alpha \pmod{a}, \quad n' \equiv \beta \pmod{b}, \quad n' \equiv \gamma \pmod{c}, \ldots$$

so wären n, n' einander kongruent nach jedem der Moduln $a, b, c, \ldots$, also auch (Nr. 1, 5) nach deren kleinstem gemeinsamen Vielfachen $a \cdot b \cdot c \ldots = m$, was sie doch als verschiedene Zahlen der Reihe (18) nicht sind. Somit ergeben die m Zahlen (18) $m = a \cdot b \cdot c \ldots$ verschiedene, d. h. alle überhaupt möglichen Restkombinationen nach den Moduln $a, b, c, \ldots$, denn bekanntlich beträgt die Anzahl der Kombinationen aus a Zahlen mit b anderen, mit c anderen Zahlen usw. ebenfalls $a \cdot b \cdot c \ldots$ Man erhält so folgenden **Satz:**

Ist $\alpha, \beta, \gamma, \ldots$ irgend eine vorgeschriebene Kombination aus den Restsystemen (22), so gibt es in der Reihe (18) eine bestimmte Zahl n, welche diese Reste läßt. Alle Zahlen, welche es ebenfalls tun, werden dann gegeben durch die Kongruenz

$$n' \equiv n \pmod{m}; \tag{23}$$

denn nur solche Zahlen n' geben, wie vorher gezeigt, dieselbe Restkombination, offenbar gibt aber auch jede mit n (mod. m) kongruente Zahl, da sie mit n auch (mod. $a, b, c, \ldots$) kongruent ist, den gleichen Rest nach diesen Moduln wie n.

Ist insbesondere n teilerfremd zu m, also auch zu $a, b, c, \ldots$, so sind auch die Reste $\alpha, \beta, \gamma, \ldots$, welche n nach diesen Moduln läßt, nach voriger Nummer teilerfremd zu $a, b, c, \ldots$ resp., wie denn auch umgekehrt, wenn die Reste $\alpha, \beta, \gamma, \ldots$ von n nach diesen Moduln prim gegen sie sind, n selbst es sein, und daher auch gegen ihr Produkt m teilerfremd sein muß. Da nun jeder Restkombination $\alpha, \beta, \gamma, \ldots$ eine und nur eine Zahl n der Reihe (18) entspricht, so muß auch die Anzahl $\varphi(m)$ der Zahlen (18), welche teilerfremd gegen m sind, der Anzahl Kombinationen aus den $\varphi(a)$ zu a, den $\varphi(b)$ zu b, den $\varphi(c)$ zu $c, \ldots$ teilerfremden Resten $\alpha, \beta, \gamma, \ldots$ gleich sein, und so ergibt sich der

Satz: Sind $a, b, c, \ldots$ zu je zweien teilerfremde Zahlen und $m = abc \ldots$, so besteht die Gleichung

$$\varphi(m) = \varphi(a) \cdot \varphi(b) \cdot \varphi(c) \ldots \tag{24}$$

Diese Eigenschaft der Funktion $\varphi(m)$ führt, wenn die Zerlegung von m in Primzahlpotenzen bekannt ist, zu einem entsprechenden Ausdrucke der Funktion, durch welchen sie berechnet werden kann. Ist nämlich

$$m = p^{\alpha} \cdot p'^{\alpha'} \cdot p''^{\alpha''} \ldots,$$

so erhält man zunächst nach dem voraufgehenden Satze

$$\varphi(m) = \varphi(p^{\alpha}) \cdot \varphi(p'^{\alpha'}) \cdot \varphi(p''^{\alpha''}) \ldots$$

Nun ist $\varphi(p^{\alpha})$ die Anzahl der Zahlen

(25) $$0, 1, 2, 3, \ldots, p^{\alpha} - 1,$$

welche prim zu p^{α}, d. h. durch p nicht teilbar sind, also offenbar gleich der gesamten Anzahl p^{α} dieser Zahlen vermindert um die Anzahl derjenigen dieser Zahlen, welche durch p teilbar sind, d. h. der Vielfachen

$$0, 1 \cdot p, 2 \cdot p, 3 \cdot p, \ldots \quad (p^{\alpha-1} - 1)p,$$

also erhält man die Gleichung

$$\varphi(p^{\alpha}) = p^{\alpha} - p^{\alpha-1} = p^{\alpha-1}(p-1).$$

Da für die übrigen Primzahlpotenzen Entsprechendes gilt, kommt endlich

(26) $$\varphi(m) = p^{\alpha-1}(p-1) \cdot p'^{\alpha'-1}(p'-1) \cdot p''^{\alpha''-1}(p''-1) \ldots$$

oder

(26a) $$\varphi(m) = m\left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{p'}\right)\left(1 - \frac{1}{p''}\right) \ldots$$

Beispiele: 1. Für $m = 12 = 2^2 \cdot 3^1$ gibt es $\varphi(12) = \varphi(2^2) \cdot \varphi(3) = 2 \cdot 2 = 4$ teilerfremde Zahlen kleiner als 12, nämlich 1, 5, 7, 11.

2. Für $m = 20$ ist $\varphi(20) = \varphi(2^2) \cdot \varphi(5) = 2 \cdot 4 = 8$, es gibt also 8 zu 20 teilerfremde Zahlen kleiner als 20, nämlich 1, 3, 7, 9, 11, 13, 17, 19.

3. Für $m = 60$ ist $\varphi(60) = \varphi(2^2) \cdot \varphi(3) \cdot \varphi(5) = 2 \cdot 2 \cdot 4 = 16$. Daher gibt es 16 zu 60 teilerfremde Zahlen kleiner als 60, nämlich

1, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53, 59.

5. Eine weitere Eigenschaft der Funktion $\varphi(m)$ liefert folgende Erwägung. Man bezeichne mit d einen Teiler von m und suche die Anzahl der Zahlen (18), welche mit m den

größten gemeinsamen Teiler d haben. Sie befinden sich natürlich alle unter den Vielfachen von d in jener Reihe, d. i. unter den Zahlen

$$0, 1 \cdot d, 2 \cdot d, 3 \cdot d, \ldots \left(\frac{m}{d} - 1\right) \cdot d;$$

irgend eins derselben, $h \cdot d$, hat aber mit $m = \frac{m}{d} \cdot d$ dann und nur dann d zum größten gemeinsamen Teiler, wenn h und $\frac{m}{d}$ teilerfremd sind. Somit ist die gesuchte Anzahl gleich der Anzahl der Zahlen

$$0, 1, 2, 3, \ldots, \frac{m}{d} - 1,$$

welche zu $\frac{m}{d}$ teilerfremd sind, d. i. gleich $\varphi\left(\frac{m}{d}\right)$.

Sind nun $1, d, d', \ldots, m$ die sämtlichen Teiler von m, so hat jede der Zahlen (18) einen dieser Teiler zum größten gemeinsamen Teiler mit m. Indem man also immer die Zahlen in eine Gruppe zusammenfaßt, denen derselbe größte gemeinsame Teiler mit m zukommt, erhält man in diesen einzelnen Gruppen bzw.

$$\varphi(m), \quad \varphi\left(\frac{m}{d}\right), \quad \varphi\left(\frac{m}{d'}\right), \quad \ldots, \quad \varphi\left(\frac{m}{m}\right)$$

Zahlen, welche zusammen alle m Zahlen (18) ergeben müssen, mithin die Gleichheit

$$(27) \qquad m = \varphi(m) + \varphi\left(\frac{m}{d}\right) + \varphi\left(\frac{m}{d'}\right) + \ldots + \varphi\left(\frac{m}{m}\right),$$

welche einfacher mittels des Summenzeichens in der Form

$$(27\text{a}) \qquad m = \sum_{d:m} \varphi\left(\frac{m}{d}\right),$$

die Summation auf alle Teiler d von m bezogen, geschrieben werden kann. Dividiert man aber m durch seine sämtlichen Teiler, so erhält man die Reihe der zu diesen komplementären Teiler, die in ihrer Gesamtheit offenbar jene Teiler in umgekehrter Reihenfolge ergeben. Man darf daher die vorstehende Gleichung auch folgendermaßen schreiben:

$$(27\text{b}) \qquad m = \varphi(1) + \varphi(d) + \varphi(d') + \cdots + \varphi(m)$$

oder den **Satz** aussprechen: **Bildet man die Funktion $\varphi(m)$ für sämtliche Teiler einer gegebenen Zahl, so ist die Summe der erhaltenen Anzahlen der letzteren Zahl gleich.**

Beispiel: Sei $m = 60$, so sind seine sämtlichen Teiler

$$d = 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60;$$

ihnen entsprechen folgende Werte

$$\varphi(d) = 1, 1, 2, 2, 4, 2, 4, 4, 8, 8, 8, 16,$$

deren Summe in der Tat gleich 60 ist.

6. Es ist nun sehr interessant, daß die in der Gleichung (27a) ausgesprochene Eigenschaft der Funktion $\varphi(m)$ ihren in (26a) gegebenen Ausdruck wieder gewinnen läßt. Sind nämlich allgemeiner $f(m)$, $\psi(m)$ zwei zahlentheoretische Funktionen, d. h. zwei Größen, welche mit der ganzen Zahl m zugleich bestimmt sind, und besteht zwischen ihnen für jeden ganzen Wert von m die der Gleichung (27a) analoge Beziehung

$$f(m) = \sum_{d:m} \psi\left(\frac{m}{d}\right), \tag{28}$$

mittels deren die f-Funktion durch ψ-Funktionen ausgedrückt wird, so läßt sich diese Beziehung umkehren, so daß die ψ-Funktion durch f-Funktionen bestimmt wird. Um diese Umkehrung zu leisten, benutzt man am besten eine ausgezeichnete zahlentheoretische Funktion, die wir

$$\mu(m)$$

nennen wollen und folgendermaßen definieren:

$\mu(m)$ sei Null, wenn m einen quadratischen Teiler hat oder, was auf dasselbe hinauskommt, wenn m wenigstens einen seiner Primfaktoren mehrfach enthält, so daß in der Zerlegung

$$m = p^{\alpha} p'^{\alpha'} \ldots p^{(k-1)\,\alpha^{(k-1)}} \tag{29}$$

mindestens einer der Exponenten größer als 1 ist; entgegengesetztenfalls, wenn also die Zerlegung von m diese wäre:

$$m = p p' \ldots p^{(k-1)}, \tag{29a}$$

sei $\mu(m) = +1$ oder -1, je nachdem die Anzahl k der verschiedenen Primfaktoren gerade oder ungerade ist; ins-

besondere setzen wir $\mu(1) = 1$. Es ist also z. B. $\mu(3) = -1$, $\mu(6) = \mu(2 \cdot 3) = +1$, $\mu(12) = \mu(2^2 \cdot 3) = 0$, usw.

Für diese Funktion $\mu(m)$ beweisen wir nun zunächst den

Satz: Ist $m > 1$, so ist die auf alle Teiler δ von m erstreckte Summe

$$\sum_{\delta : m} \mu(\delta) = 0. \tag{30}$$

Da $\mu(\delta)$ für diejenigen Teiler δ von m Null ist, welche einen mehrfachen Primteiler haben, genügt es, die Summe auf die übrigen δ zu erstrecken; da aber ein Teiler δ von m keine anderen Primfaktoren haben kann als m selbst, weil ja jeder Teiler von δ auch ein solcher von m ist, kann δ nur die Form haben

$$\delta = p^{\beta} p'^{\beta'} \ldots \; p^{(k-1)\,\beta^{(k-1)}},$$

wo die Exponenten Null oder positive ganze Zahlen sind, und δ wird dann und nur dann ohne mehrfache Primfaktoren sein, wenn keiner der Exponenten größer als 1 ist. Die vorher gedachten übrigen Teiler δ von m sind also nur die folgenden:

Die Zahl: 1,

die einzelnen Primzahlen: $p, p', p'', \ldots, p^{(k-1)}$,

die Produkte aus je zwei derselben: $pp', pp'', p'p'', \ldots$,

die Produkte aus je drei derselben: $pp'p'', pp'p''', p'p''p''', \ldots$,

. . . .

endlich das Produkt: $pp'p'' \ldots p^{(k-1)}$.

Die Anzahl der Zahlen δ in diesen einzelnen Reihen beträgt

$$1, \quad \frac{k}{1}, \quad \frac{k(k-1)}{1 \cdot 2}, \quad \frac{k(k-1)(k-2)}{1 \cdot 2 \cdot 3}, \quad \ldots, \quad 1$$

und, weil $\mu(\delta)$ entsprechend den aufeinanderfolgenden Reihen gleich $+1, -1, +1, \ldots, (-1)^k$ ist, erhält man für die Summe (30) folgenden Wert:

$$1 - \frac{k}{1} + \frac{k(k-1)}{1 \cdot 2} - \frac{k(k-1)(k-2)}{1 \cdot 2 \cdot 3} + \ldots + (-1)^k,$$

d. h. $(1-1)^k$ also, wenn $k \geqq 1$, gleich Null, w. z. b. w.

Nachdem dies bewiesen worden, bezeichnen wir jetzt wieder mit δ jeden Teiler von m und multiplizieren die der Gleichung (28) entsprechende Gleichung

$$f\left(\frac{m}{\delta}\right) = \sum_{d:\frac{m}{\delta}} \psi\left(\frac{m}{d\,\delta}\right),$$

in welcher die Summe zur Rechten nunmehr auf alle Teiler d von $\frac{m}{\delta}$ zu erstrecken ist, mit $\mu(\delta)$, und summieren dann über alle Werte von δ. So erhalten wir

$$\text{(31)} \qquad \sum_{\delta:m} \mu(\delta) \cdot f\left(\frac{m}{\delta}\right) = \sum_{\delta:m} \left(\sum_{d:\frac{m}{\delta}} \mu(\delta) \cdot \psi\left(\frac{m}{d\delta}\right)\right).$$

Durchläuft aber δ die Teiler von m und d jedesmal alle Teiler von $\frac{m}{\delta}$, so ist jedesmal auch $d\delta$ ein Teiler von m, auch erhält man so alle Teiler von m, da z. B. für $\delta = 1$ das Produkt $d\delta = d$ alle Teiler von $\frac{m}{1}$ anzunehmen hat. Vereinigt man daher in der Doppelsumme zur Rechten alle Glieder, in welchen sich das Produkt $d\delta$ zu ein und demselben Teiler t von m zusammenfaßt: $d\delta = t$, wobei δ offenbar alle Teiler von t durchläuft, so kann man die Doppelsumme auch folgendermaßen schreiben:

$$\sum_{t:m} \left(\psi\left(\frac{m}{t}\right) \cdot \sum_{\delta:t} \mu(\delta) \right),$$

und man erhält, da mit Rücksicht auf den Satz (30) nur ihr, dem Werte $t = 1$ entsprechendes Glied stehen bleibt, dafür den einfachen Wert $\psi(m)$. Demnach geht aus (31) die erwähnte Umkehrungsformel

$$\text{(32)} \qquad \psi(m) = \sum_{\delta:m} \mu(\delta) \cdot f\left(\frac{m}{\delta}\right)$$

hervor.

Im besonderen folgt also aus (27a) die Beziehung

$$\varphi(m) = \sum_{\delta:m} \mu(\delta) \cdot \frac{m}{\delta},$$

d. i. mit Beachtung des beim Beweise der Formel (30) Bemerkten

$$\varphi(m)=m-m\left(\frac{1}{p}+\frac{1}{p'}+\frac{1}{p''}+\cdots\right)+m\left(\frac{1}{pp'}+\frac{1}{pp''}+\frac{1}{p'p''}+\cdots\right)$$
$$-m\left(\frac{1}{pp'p''}+\frac{1}{pp'p'''}+\frac{1}{p'p''p'''}+\cdots\right)+\cdots$$
$$+(-1)^k\cdot\frac{m}{pp'\ldots p^{(k-1)}},$$

was nichts anderes ist als die entwickelte Formel (26a):

$$\varphi(m)=m\left(1-\frac{1}{p}\right)\left(1-\frac{1}{p'}\right)\cdots\left(1-\frac{1}{p^{(k-1)}}\right).$$

7. Wird ein vollständiges Restsystem

(33) $$r_0, r_1, r_2, \ldots, r_{m-1} \pmod{m}$$

mit irgend einer zu m teilerfremden Zahl ϱ multipliziert, so entstehen m untereinander inkongruente Zahlen

(33a) $$\varrho r_0, \varrho r_1, \varrho r_2, \ldots, \varrho r_{m-1},$$

denn aus der Kongruenz $\varrho r_i \equiv \varrho r_k$ zweier von ihnen ergäbe sich, da ϱ relativ prim zu m ist, die Kongruenz $r_i \equiv r_k$, während die Zahlen (33) als inkongruent gedacht sind. Demnach bilden die Zahlen (33a) wieder ein vollständiges Restsystem (mod. m) und müssen, von der Ordnung abgesehen, den Zahlen (33) insgesamt kongruent sein. Es gibt also immer eine Zahl r der Reihe (33), für welche ϱr einer beliebig gewählten Zahl der Reihe (33) oder, da jede Zahl n einer von diesen kongruent ist, einer ganz beliebig gewählten Zahl n kongruent wird (mod. m), mit anderen Worten: Die Kongruenz ersten Grades

(34) $$\varrho x \equiv n \pmod{m}$$

hat stets eine Auflösung, wenn der Koeffizient ϱ teilerfremd zum Modul ist. — Ist aber $x = r$ eine Auflösung, so gibt es unendlich viele, die alle durch die Formel $x \equiv r$ (mod. m) bestimmt sind, denn mit r leistet auch jede ihr kongruente Zahl der Kongruenz Genüge; aber auch umgekehrt jede ihr genügende Zahl r' muß mit r kongruent sein, da aus

$$\varrho r \equiv n, \quad \varrho r' \equiv n$$

sich

$$\varrho r \equiv \varrho r',$$

also auch $r \equiv r'$ (mod. m) ergibt. Die Kongruenz (34) hat also eine und nur eine Wurzel.

Beispiel. Sei zu lösen $7x \equiv -8$ (mod. 12). Multipliziert man die Reste

$$0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10,\ 11$$

mit 7, so erhält man für die Vielfachen die folgenden Reste:

$$0,\ 7,\ 2,\ 9,\ 4,\ 11,\ 6,\ 1,\ 8,\ 3,\ 10,\ 5,$$

von welchen $4 \equiv -8$ (mod. 12) ist, also ist die Lösung

$$x \equiv 4 \quad (\text{mod. } 12),$$

wofür in der Tat $7 \cdot 4 \equiv -8$ oder $7 \cdot 4 + 8 = 36$ durch 12 teilbar ist.

Anders ist es mit der Kongruenz

$$(34\text{a}) \qquad \varrho x \equiv n \quad (\text{mod. } m),$$

wenn der Koeffizient ϱ nicht teilerfremd zu m ist, sondern einen von 1 verschiedenen größten gemeinsamen Teiler δ mit dem Modul m hat. Setzt man dann nämlich $\varrho = \delta\varrho'$, $m = \delta m'$, wo nun ϱ', m' teilerfremde ganze Zahlen sind, so müßte, wenn die Kongruenz (34a) stattfände, n, als derselben Klasse angehörig wie $\varrho x = \delta \cdot \varrho' x$, ebenfalls mit m den gemeinsamen Teiler δ haben, so daß $n = \delta n'$ gesetzt werden könnte. Andernfalls, wenn nämlich n nicht durch den größten gemeinsamen Teiler des Koeffizienten ϱ und des Moduls m teilbar ist, wird die Kongruenz (34a) unlösbar sein. Dagegen folgt, wenn n durch diesen größten gemeinsamen Teiler aufgeht, aus

$$\varrho x - n = \delta \cdot (\varrho' x - n'),$$

daß zugleich mit $\varrho x - n$ auch $(\varrho' x - n')\,\delta$ durch $m = m'\delta$, also $\varrho' x - n'$ durch m' aufgeht, oder es folgt aus der Kongruenz (34a) die andere:

$$\varrho' x \equiv n' \quad (\text{mod. } m');$$

jede Lösung der ersteren ist also auch eine solche der letzteren. Diese hat aber, da ϱ', m' teilerfremd sind, eine

Wurzel $x \equiv r \pmod{m'}$, und für jeden solchen Wert von x ist auch wirklich
$$\varrho x - n = \delta(\varrho' x - n')$$
teilbar durch m, da $\varrho' x - n' \equiv \varrho' r - n' \pmod{m'}$, d. h. durch m' teilbar ist. Alle diese Zahlen x sind durch die Formel

$$x = r + m' z \tag{35}$$

gegeben, wenn darin z alle ganzen Zahlen durchläuft; dies geschieht aber nach der Grundtatsache der Zahlentheorie, wenn $z = \delta y + t$ gesetzt wird und y alle ganzen Zahlen, t aber alle Zahlen $0, 1, 2, \ldots, \delta - 1$ durchläuft. Somit erhält man aus (35) die Formel

$$x = (r + m't) + my,$$

oder die δ verschiedenen Formeln

$$\left.\begin{cases} x \equiv r \\ x \equiv r + m' \\ x \equiv r + 2m' \\ \cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot \\ x \equiv r + (\delta - 1)m' \end{cases}\right\} \pmod{m}, \tag{36}$$

welche alle Auflösungen von (34a) liefern und offenbar δ Wurzeln $(\text{mod.}\, m)$ repräsentieren, da je zwei der Werte

$$r,\quad r + m',\quad r + 2m',\quad \ldots,\quad r + (\delta - 1)m'$$

eine durch m nicht teilbare Differenz ergeben. Es gilt daher der

Satz: Ist für die Kongruenz (34a), in welcher ϱ und m den größten gemeinsamen Teiler δ haben, die notwendige Bedingung, daß auch n durch δ teilbar sei, erfüllt, so hat die Kongruenz δ Wurzeln.

Beispiele: 1. $8x \equiv 5 \pmod{12}$ ist unmöglich, denn 5 geht durch den größten gemeinsamen Teiler 4 von 8 und 12 nicht auf.

2. $8x \equiv 4 \pmod{12}$ gibt $2x \equiv 1 \pmod{3}$, eine Kongruenz, der durch $x \equiv 2 \pmod{3}$, d. h. $x = 2 + 3 \cdot z$ oder
$$x = 2 + 3(t + 4y) \equiv 2 + 3t \pmod{12}$$
genügt wird; die gegebene Kongruenz hat also die Wurzeln
$$x \equiv 2, \quad x \equiv 5, \quad x \equiv 8, \quad x \equiv 11 \pmod{12}.$$

8. Denkt man sich jetzt statt eines vollständigen Restsystems nur die Glieder eines reduzierten Restsystems

(37) $$\varrho_1, \varrho_2, \varrho_3, \ldots, \varrho_\mu$$

(mod. m) mit irgend einer zu m teilerfremden Zahl ϱ multipliziert, so erhält man der vorigen Nummer zufolge μ (mod. m) inkongruente Produkte

(37a) $$\varrho\varrho_1, \varrho\varrho_2, \varrho\varrho_3, \ldots, \varrho\varrho_\mu,$$

die zugleich auch zu m teilerfremd sind, da die Faktoren es sind. Diese Produkte bilden daher wieder ein reduziertes Restsystem (mod. m) und müssen also, von der Ordnung abgesehen, den Zahlen (37) kongruent sein, so daß auch das Produkt der Zahlen (37a) demjenigen der letzteren Zahlen kongruent sein muß, in Zeichen:

$$\varrho^\mu \cdot \varrho_1 \varrho_2 \cdots \varrho_\mu \equiv \varrho_1 \varrho_2 \cdots \varrho_\mu \pmod{m}.$$

Da jedoch mit den Zahlen $\varrho_1, \varrho_2, \ldots, \varrho_\mu$ auch deren Produkt zum Modul teilerfremd ist, läßt der gleiche Faktor beider Seiten sich heben und für jede zu m teilerfremde Zahl ϱ die Kongruenz

$$\varrho^\mu \equiv 1 \pmod{m}$$

oder mit Benutzung des Funktionszeichens $\varphi(m)$ für μ die Kongruenz

(38) $$\varrho^{\varphi(m)} \equiv 1 \pmod{m}$$

sich erschließen. Da diese Kongruenz, die hier für jede zu m teilerfremde Zahl ϱ bewiesen ist, für eine Zahl ϱ, welche irgend einen Teiler mit m gemeinsam hat, nicht bestehen kann, da die rechte Seite ihn nicht auch hat, erkennt man weiter den

Satz: Die Kongruenz

(38a) $$x^{\varphi(m)} \equiv 1 \pmod{m}$$

hat genau soviel Wurzeln als ihr Grad beträgt, und sie werden durch sämtliche Glieder eines reduzierten Restsystems (mod. m) repräsentiert.

Die Kongruenz (38) ist die durch *Euler* gegebene Verallgemeinerung eines Satzes, den man unter vielen anderen wichtigen zahlentheoretischen Sätzen dem Vater der modernen Zahlentheorie, dem berühmten französischen Mathe-

matiker des 17. Jahrhunderts, *Pierre Fermat*, verdankt und welcher daher als **Fermatscher Satz** benannt wird. Man erhält diesen, wenn man den Modul m als Primzahl p voraussetzt, wo dann $\varphi(m) = \varphi(p) = p - 1$ wird und die Kongruenz (38) die Form annimmt

(39) $$\varrho^{p-1} \equiv 1 \pmod{p}.$$

In Worten: Jede durch die Primzahl p nicht teilbare Zahl gibt, zur $p-1$ten Potenz erhoben, den Rest 1 (mod. p).

Aus (39) folgt durch Multiplikation mit ϱ die andere Kongruenz

(40) $$\varrho^{p} \equiv \varrho \pmod{p},$$

die den Vorzug genießt, daß sie offenbar auch für Zahlen, welche durch p teilbar sind, also für jedwede Zahl ϱ gilt, während für solche, die nicht durch p teilbar sind, daraus wieder die Kongruenz (39) hervorgeht. Wir können also den *Fermat*schen Satz vorteilhafter auch so aussprechen:

Ist p eine Primzahl, so ist die $p$te Potenz jeder Zahl mit dieser Zahl selbst (mod. p) kongruent.

Beispiele:

1. Für $m = 60$ ist $\varphi(m) = 16$; man findet

$7^1 \equiv 7, \quad 7^2 = 49 \equiv -11, \quad 7^3 \equiv -77 \equiv -17,$

$7^4 \equiv -119 \equiv +1$, also auch $7^{16} \equiv 1$.

$11^1 \equiv 11, \quad 11^2 = 121 \equiv 1$, also auch $11^{16} \equiv 1$.

$23^1 \equiv 23, \; 23^2 = 529 \equiv 49 \equiv -11, \; 23^3 \equiv -253 \equiv -13,$

$23^4 \equiv -299 \equiv -59 \equiv 1$, also auch $23^{16} \equiv 1 \pmod{60}$.

2. Für $m = p = 11$ findet man

$2^1 \equiv 2, \; 2^2 \equiv 4, \; 2^3 \equiv 8, \; 2^4 \equiv 16 \equiv 5, \; 2^5 \equiv 10 \equiv -1,$ also $2^{10} \equiv +1 \pmod{11}$.

$3^1 \equiv 3, \quad 3^2 \equiv 9, \quad 3^3 \equiv 5, \quad 3^4 \equiv 4, \quad 3^5 \equiv 1,$ also auch $3^{10} \equiv 1 \pmod{11}$.

$7^1 \equiv 7, \quad 7^2 \equiv 5, \quad 7^3 \equiv 35 \equiv 2, \quad 7^4 \equiv 14 \equiv 3,$

$7^5 \equiv 21 \equiv -1$, also auch $7^{10} \equiv 1 \pmod{11}$.

3. Bildet man für den Modul $m = p = 19$ die Reste der aufeinanderfolgenden Potenzen der Zahlen

$$1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10,\ 11,\ 12,\ 13,\ 14,\ 15,\ 16,\ 17,\ 18,$$

so findet man, daß zuerst die Potenzen

$$1^1,\ 2^{18},\ 3^{18},\ 4^9,\ 5^9,\ 6^9,\ 7^3,\ 8^6,\ 9^9,\ 10^{18},\ 11^3,\ 12^6,\ 13^{18},\ 14^{18},\ 15^{18},\ 16^9,\ 17^9,\ 18^2$$

den Rest 1 lassen. Folglich ist, da die Exponenten 1, 2, 3, 6, 9, 18 sämtlich Teiler von 18 sind, die 18te Potenz jeder der durch 19 nicht teilbaren Zahlen kongruent 1 (mod. 19).

9. Sei jetzt p eine ungerade Primzahl, die wir zunächst größer als 3 voraussetzen. Da die $p-1$te Potenz jeder durch p nicht teilbaren Zahl ϱ der Eins kongruent ist (mod. p), so gibt es auch eine kleinste positive Potenz von dieser Beschaffenheit. Ist ϱ^d diese kleinste Potenz, also $\varrho^d \equiv 1$ (mod. p), dagegen nicht $\varrho^c \equiv 1$, wenn $c < d$ (außer für $c = 0$), so sagt man, ϱ gehöre (mod. p) zum Exponenten d. Dieser Exponent ist stets ein Teiler von $p-1$. Es leuchtet nämlich ein, daß stets $\varrho^n \equiv 1$ ist, wenn n durch d teilbar, $n = qd$ ist, denn dann ist $\varrho^n = (\varrho^d)^q \equiv 1$ (mod. p), daß dagegen ϱ^n nicht $\equiv 1$ sein kann, wenn der Exponent n nicht durch d teilbar, also von der Form $n = qd + c$ ist, wo c eine der Zahlen $0, 1, 2, \ldots, d-1$, denn dann wäre

$$\varrho^n = \varrho^{qd} \cdot \varrho^c \equiv \varrho^c \equiv 1$$

gegen die Bedeutung des Exponenten d. Da nun $\varrho^{p-1} \equiv 1$ ist, muß, wie behauptet, $p-1$ teilbar sein durch d.

Entweder ist nun für eine bestimmte Zahl ϱ der Exponent d, zu dem sie gehört, gleich $p-1$, also eine Zahl vorhanden, welche zu dem größtmöglichen Exponenten $p-1$ gehört, oder d ist ein echter Teiler von $p-1$ und dann d, ja sogar $d+1 < p-1$. Da es nur einen zum Exponenten 1 gehörigen, d. h. die Kongruenz $x^1 \equiv 1$ (mod. p) befriedigenden Rest, nämlich den Rest 1 (mod. p) gibt, und da alle zu d oder einem Teiler von d gehörigen inkongruenten Zahlen x der Kongruenz $x^d \equiv 1$ (mod. p) genügen, welche höchstens

d Wurzeln hat, so muß es wegen $d+1<p-1$ eine Zahl ϱ' geben, die zu einem Exponenten d' gehört, welcher von 1 und d verschieden, auch kein Teiler von d ist. Dann sei δ der größte gemeinsame Teiler von d, d', so daß $d=\delta e$, $d'=\delta e'$ gesetzt werden kann, wo e, e' relativ prim sind, und das kleinste gemeinsame Vielfache der beiden Exponenten

$$\mu=\frac{d\,d'}{\delta}=\delta\,e\,e'$$

größer als d ist. Die Primfaktoren von δ gehen entweder in e oder in e' oder in keiner dieser Zahlen auf; wir nennen die der ersteren Art $p, \ldots$, die der zweiten $p', \ldots$, die der dritten $p'', \ldots$, und bezeichnen mit

$$p^{a}, \ldots; \quad p'^{a'}, \ldots; \quad p''^{a''}, \ldots$$

die entsprechenden, in δ aufgehenden Potenzen derselben. Zieht man die ersteren zum Faktor e, die zweiten zum Faktor e', die letzten nach Belieben zu jenem oder zu diesem hinzu, so erhält man μ als Produkt von zwei teilerfremden Faktoren:

$$\mu=\theta\,e\cdot\theta'\,e',$$

während $\theta\,\theta'=\delta$ ist. Mit Hilfe dieser Bemerkung läßt sich zeigen, daß das kleinste gemeinsame Vielfache μ der Exponent ist, zu welchem die Zahl

$$\varrho^{\theta'}\cdot\varrho'^{\theta}$$

gehört. In der Tat ist zunächst

$$(\varrho^{\theta'}\cdot\varrho'^{\theta})^{\mu}=(\varrho^{d})^{e'\theta'}\cdot(\varrho'^{d'})^{e\theta}\equiv 1 \pmod{p}.$$

Daher muß der Exponent, zu welchem die gedachte Zahl gehört, ein Teiler von μ, d. h. von der Form $\eta\cdot\eta'$ sein, wo η, η' resp. aufgehen in θe, $\theta' e'$. Da also $(\varrho^{\theta'}\cdot\varrho'^{\theta})^{\eta'\eta}\equiv 1$ ist, müssen auch

$$(\varrho^{\theta'}\varrho'^{\theta})^{\theta e\eta'}=(\varrho^{d})^{\eta'}\cdot\varrho'^{\theta^2 e\eta'}\equiv\varrho'^{\theta^2 e\eta'}\equiv 1$$
$$(\varrho^{\theta'}\varrho'^{\theta})^{\theta' e'\eta}=(\varrho'^{d'})^{\eta}\cdot\varrho^{\theta'^2 e'\eta}\equiv\varrho^{\theta'^2 e'\eta}\equiv 1$$

sein, woraus sich $\theta^2 e\eta'$ durch $d'=\theta\,\theta' e'$, d. h. $\theta e\eta'$ durch $\theta' e'$, also η' durch $\theta' e'$ und ebenso $\theta'^2 e'\eta$ durch $d=\theta\,\theta' e$, d. h. $\theta' e'\eta$ durch θe, also η durch θe teilbar ergibt, was nur sein kann, wenn $\eta=\theta e$, $\eta'=\theta' e'$, mithin der Exponent $\eta\,\eta'$, zu welchem $\varrho^{\theta'}\cdot\varrho'^{\theta}$ gehört, gleich $\theta e\cdot\theta' e'=\mu$ ist.

So sind wir zu einer Zahl gelangt, für welche der Exponent, zu dem sie gehört, größer ist als d. Ist er noch kleiner als $p-1$, so kann man, von ihm ausgehend, das gleiche Räsonnement wiederholen und eine zu einem noch größeren Exponenten gehörige Zahl ermitteln usw., so daß man notwendig zuletzt eine zum Exponenten $p-1$ gehörige Zahl findet.

Hierdurch haben wir die wichtige Tatsache festgestellt, daß es stets Zahlen gibt, die zum Exponenten $p-1$ (mod. p) gehören, und zugleich einen Weg aufgezeigt, um eine solche Zahl zu ermitteln. In dem bisher ausgeschlossenen Falle $p=3$ ist die Existenz einer solchen Zahl ersichtlich, da offenbar 2 zum Exponenten 2 (mod. 3) gehört; in der Tat ist $2^1 \equiv 2$, $2^2 = 4 \equiv 1$ (mod. 3).

Z. B. fanden wir, daß 7^3 die kleinste Potenz von 7 ist, welche (mod. 19) den Rest 1 läßt oder daß 7 (mod. 19) zum Exponenten 3 gehört; die Zahl 18 gehört desgleichen zum Exponenten 2, daher wird

$$7^2 \cdot 18^3 \equiv 49 \cdot 18 \equiv -11 \equiv 8 \quad (\text{mod.}\, 19)$$

zum Exponenten $2 \cdot 3 = 6$ gehören. Ferner gehört 5 zum Exponenten 9; das kleinste gemeinsame Vielfache von 6 und 9 ist $18 = 2\theta \cdot 3\theta'$, wo $\theta\theta' = 3$, also etwa $\theta = 1$, $\theta' = 3$ ist; demnach gehört $8^3 \cdot 5^1 \equiv -5 \equiv 14$ (mod. 19) zum Exponenten 18, wie das Beispiel 3. voriger Nummer bestätigt.

10. Man kann dieselbe Tatsache auch folgendermaßen feststellen. Da jeder der Reste $1, 2, 3, \ldots, p-1$ (mod. p) zu einem bestimmten Exponenten d gehört, der ein Teiler von $p-1$ ist, so kann man jene Reste in Gruppen verteilen, indem man immer diejenigen Reste in eine Gruppe vereint, die zu demselben Teiler von $p-1$ gehören. Nennt man also $1, d, d', \ldots, p-1$ die sämtlichen Teiler von $p-1$ und bezeichnet allgemein mit $\psi(d)$ die Anzahl derjenigen Reste, die zum Teiler d als Exponenten gehören, wobei möglicherweise $\psi(d)$ Null, niemals aber negativ sein kann, so muß offenbar die Gesamtsumme der in den einzelnen Gruppen enthaltenen Reste

$$\psi(1) + \psi(d) + \psi(d') + \ldots + \psi(p-1) = p-1$$

sein. Nun besteht aber für die φ-Funktion nach *nr* $\cdot$ 5 die völlig entsprechende Gleichheit

$$\varphi(1) + \varphi(d) + \varphi(d') + \ldots + \varphi(p-1) = p-1.$$

Kann man also zeigen, daß immer $\psi(d) \gtreqless \varphi(d)$ ist, so muß allgemein $\psi(d) = \varphi(d)$ sein, denn, wäre auch nur für einen einzigen Teiler von $p-1$ das Gegenteil der Fall, so müßte die erstere Summe geringer ausfallen als die zweite, die doch den gleichen Wert besitzt wie sie. Dies läßt sich folgendermaßen erkennen. Gibt es überhaupt eine zum Exponenten d gehörige Zahl ϱ, so sind die Potenzen $1, \varrho, \varrho^2, \ldots, \varrho^{d-1}$ die Wurzeln der Kongruenz

$$(41) \qquad x^d \equiv 1 \pmod{p},$$

denn erstens sind sie inkongruent, da aus einer Kongruenz $\varrho^h \equiv \varrho^k$, wo $h < k$ gedacht werde, sich ϱ^{k-h}, d. h. eine kleinere als die $d$te Potenz von ϱ der Eins kongruent ergäbe gegen die Bedeutung von d; zweitens ist zugleich mit ϱ auch jede jener Potenzen eine Wurzel von (41), da

$$(\varrho^h)^d = (\varrho^d)^h \equiv 1 \pmod{p};$$

und drittens hat die Kongruenz (41) nicht mehr als d Wurzeln. Unter den gedachten d Potenzen von ϱ befinden sich also auch alle Zahlen eines Restsystems, welche zum Exponenten d gehören; ist aber in ϱ^h der Exponent h nicht relativ prim zu d, sondern $\delta > 1$ ein gemeinsamer Teiler von h und d, so ist bereits

$$(\varrho^h)^{\frac{d}{\delta}} = (\varrho^d)^{\frac{h}{\delta}} \equiv 1 \pmod{p},$$

also gehört dann ϱ^h nicht zum Exponenten d; demnach können nur diejenigen $\varphi(d)$ der Potenzen ϱ^h, deren Exponent h teilerfremd ist zu d, zum Exponenten d gehören, und die Anzahl $\psi(d)$ der zum Exponenten d gehörigen Reste ist daher, wenn nicht Null, doch, was zu zeigen war, nicht größer als $\varphi(d)$.

Wird dies insbesondere auf den Teiler $d = p-1$ angewandt, so bestätigt sich nicht nur die vorher auf anderem Wege erhaltene Tatsache von dem Vorhandensein einer zum Exponenten $p-1$ gehörigen Zahl, sondern es stellt sich auch heraus, daß es $\varphi(p-1)$ inkongruente Zahlen dieser Art gibt.

Man nennt jede solche Zahl eine primitive Wurzel der Kongruenz

$$x^{p-1} \equiv 1 \pmod{p}$$

oder kürzer eine primitive Wurzel (mod. p). Dem eben Bewiesenen zufolge gibt es $\varphi(p-1)$ inkongruente primitive Wurzeln.

In Beispiel 3. Nr. 8 sind die angegebenen Potenzen der Zahlen 1, 2, 3, ..., die (mod. 19) den Rest 1 lassen, zugleich die niedrigsten Potenzen dieser Art, also gehören zu den Teilern 1, 2, 3, 6, 9, 18 der Zahl 18 resp. 1, 1, 2, 2, 6, 6 Reste, welche Zahlen in der Tat mit $\varphi(1)$, $\varphi(2)$, $\varphi(3)$, $\varphi(6)$, $\varphi(9)$, $\varphi(18)$ übereinstimmen; es gibt $6=\varphi(18)$ primitive Wurzeln 2, 3, 10, 13, 14, 15.

11. Bedeutet g irgend eine primitive Wurzel (mod. p), so sind alle Potenzen

$$g^0=1,\ g,\ g^2,\ \ldots,\ g^{p-2} \tag{42}$$

(mod. p) inkongruent und stellen daher ein reduziertes Restsystem für diesen Modul dar. In der Tat sind alle diese Potenzen zugleich mit g teilerfremd gegen p und zwei verschiedene derselben können nicht kongruent sein, da aus $g^h \equiv g^k$ (mod. p), wo $h<k<p-1$ gedacht wird, sich $g^{k-h}\equiv 1$ ergäbe, während $k-h<p-1$ wäre, gegen die Bedeutung von g.

Hieraus folgt, daß jede durch p nicht teilbare Zahl r einer bestimmten Potenz aus der Reihe (42) kongruent sein muß (mod. p). Ist g^i diese Potenz, also

$$r\equiv g^i \pmod{p}, \tag{43}$$

so heißt i der Index der Zahl r, in Zeichen: $i=\text{ind.}\,r$. Für solche Indizes gilt der **Satz:** daß der Index eines Produktes der Summe der Indizes der Faktoren (mod. $p-1$) kongruent, nämlich ihr kleinster positiver Rest (mod. $p-1$) ist, so daß, wenn r, r' zwei durch p nicht teilbare Zahlen bedeuten,

$$\text{ind.}\,r\,r' \equiv \text{ind.}\,r + \text{ind.}\,r' \pmod{p-1} \tag{44}$$

ist. In der Tat bestehen der Bedeutung des Index zufolge die beiden Kongruenzen

$$r\equiv g^{\text{ind.}\,r},\quad r'\equiv g^{\text{ind.}\,r'} \pmod{p},$$

aus denen die dritte

$$r\,r' \equiv g^{\text{ind.}\,r+\text{ind.}\,r'} \pmod{p}$$

folgt. Da nun zugleich auch

$$r r' \equiv g^{\text{ind.} r r'} \pmod{p}$$

ist, müssen die beiden Potenzen

$$g^{\text{ind.} r r'}, \quad g^{\text{ind.} r + \text{ind.} r'}$$

der primitiven Wurzel einander kongruent sein. Allgemein folgt aber aus $g^m \equiv g^n \pmod{p}$, wenn etwa $m > n$ ist, $g^{m-n} \equiv 1 \pmod{p}$, mithin $m - n$ als Vielfaches des Exponenten $p-1$, zu welchem g gehört. Daher muß auch die Differenz der beiden Zahlen ind.$r r'$, ind.r + ind.r' durch $p-1$ teilbar, d. h. die Kongruenz (44) erfüllt sein.

Beispiel. Für $p = 19$ ist $g = 2$ eine primitive Wurzel und man findet für

$$\begin{array}{rcccccccccccccccccccc} h & = & 0, & 1, & 2, & 3, & 4, & 5, & 6, & 7, & 8, & 9, & 10, & 11, & 12, & 13, & 14, & 15, & 16, & 17, & 18 \\ 2^h & \equiv & 1, & 2, & 4, & 8, & 16, & 13, & 7, & 14, & 9, & 18, & 17, & 15, & 11, & 3, & 6, & 12, & 5, & 10, & 1, \end{array}$$

also

$$\text{ind.} h = 0, 1, 13, 2, 16, 14, 6, 3, 8, 17, 12, 15, 5, 7, 11, 4, 10, 9;$$

hieraus findet man z. B.

$$\left.\begin{array}{l} \text{ind.} 12 \equiv \text{ind.} 3 + \text{ind.} 4 \equiv 13 + 2 \equiv 15 \\ \text{ind.} 18 \equiv \text{ind.} 3 + \text{ind.} 6 \equiv 13 + 14 \equiv 27 \equiv 9 \end{array}\right\} \pmod{18}.$$

Man ersieht aus der Definition des Index, daß derselbe nicht absolut bestimmt, sondern nur bezüglich auf eine gegebene primitive Wurzel und von dieser, welche der Betrachtung zugrunde gelegt wird, abhängig ist, und deshalb genauer unter Andeutung dieser Wurzel etwa mit $\text{ind.}_g r$ zu bezeichnen wäre. In der Tat, wenn statt g eine andere primitive Wurzel γ gewählt wird, so findet man gleicherweise

$$r \equiv \gamma^{i'} \pmod{p},$$

wo i' eine Zahl der Reihe $0, 1, 2, 3, \ldots, p-1$ und bei entsprechender Bezeichnung $i' = \text{ind.}_\gamma r$ ist. Bedenkt man, daß auch γ als eine durch p nicht teilbare Zahl einen mit Bezug auf g genommenen Index $c = \text{ind.}_g \gamma$ besitzt, demzufolge

$$\gamma \equiv g^c \pmod{p}$$

gesetzt werden darf, so schreibt sich die voraufgehende Kongruenz wie folgt:

$$r \equiv g^{c i'} \pmod{p}$$

und gibt mit (43) verbunden die andere

$$g^{i} \equiv g^{c i'} \quad (\text{mod.} p),$$

aus welcher einer voraufgehenden allgemeinen Bemerkung gemäß

$$i \equiv c i' \quad (\text{mod.} p-1),$$

d. i. die Kongruenz

$$\text{ind.}_g r \equiv \text{ind.}_g \gamma \cdot \text{ind.}_\gamma r \quad (\text{mod.} p-1)$$

hervorgeht. Diese Kongruenz zeigt an, wie man aus dem auf eine bestimmte primitive Wurzel γ bezüglichen Index einer Zahl r den auf eine andere primitive Wurzel g bezüglichen Index derselben Zahl ermitteln kann; man hat nur den ersteren mit dem Index von γ in bezug auf g zu multiplizieren und den kleinsten positiven Rest des Produktes (mod. $p-1$) zu nehmen. Hierin tritt ebenso wie in der Kongruenz (44) eine augenscheinliche Analogie zwischen der Theorie der Indizes und derjenigen der Logarithmen zutage.

Beispiel. Für $p = 19$ ist neben 2 auch 3 eine primitive Wurzel; um aus den vorher für die erstere angegebenen Werten von $\text{ind.}_2 h$ die von $\text{ind.}_3 h$ zu finden, suche man $\text{ind.}_3 2$, d. i. die Potenz 3^x, welche kongruent 2 ist (mod. 19); man findet leicht $x = 7 = \text{ind.}_3 2$; multipliziert man also die angegebenen Werte von ind. h mit 7 und nimmt die kleinsten positiven Reste (mod. 18), so erhält man

$$\text{ind.}_3 h = 0, 7, 1, 14, 4, 8, 6, 3, 2, 11, 12, 15, 17, 13, 5, 10, 16, 9.$$

Drittes Kapitel.

Von den quadratischen Resten.

1. Der *Fermat*sche Lehrsatz bildet den Zugang zur Lehre von den Potenzresten, d. i. zur Untersuchung der Frage, ob eine gegebene ganze Zahl a in bezug auf einen gegebenen Modul m der Potenz einer Zahl von vorgeschriebenem Grade n kongruent sein kann oder nicht, ob also, mit anderen Worten, die sogenannte binomische Kongruenz

$$x^n \equiv a \quad (\text{mod.} m)$$

lösbar ist oder nicht. Wir wollen hier diese Untersuchung nur für quadratische Kongruenzen, d. h. für $n = 2$ und ausschließlich für den Fall führen, daß der Modul m eine ungerade Primzahl p ist. Je nachdem dann die Kongruenz

$$(1) \qquad x^2 \equiv a \pmod{p}$$

lösbar ist oder nicht, werde a ein quadratischer Rest oder ein quadratischer Nichtrest — kürzer ein Nichtrest (mod. p) genannt. Da die Kongruenz, falls a durch p teilbar wäre, offenbar für jeden durch p teilbaren Wert von x befriedigt würde, beschränken wir uns ferner auf die Voraussetzung, daß a durch p nicht teilbar sei.

Wir beginnen mit der Bemerkung, daß, wenn die Kongruenz (1) lösbar ist, sie genau zwei Wurzeln, d. i. zwei inkongruente Lösungen besitzt. Daß sie nicht mehr als zwei haben kann, folgt aus dem allgemeinen Satze in Nr. 2 des vorigen Kapitels über die mögliche Anzahl der Wurzeln einer Kongruenz (mod. p). Ist aber $x \equiv \alpha$ (mod. p) eine Wurzel, also $\alpha^2 \equiv a$ (mod. p), so ist auch $x \equiv -\alpha$ eine solche, da $(-\alpha)^2 = \alpha^2 \equiv a$ ist, und zwar eine zweite Wurzel, da die Zahlen α, $-\alpha$ einander nicht kongruent sein können; in der Tat kann ihre Differenz 2α nicht durch p teilbar sein, da weder 2 noch α durch p aufgeht, letzteres deshalb nicht, weil sonst wegen $\alpha^2 \equiv a$ auch a durch p teilbar wäre, was gegen die Voraussetzung ist.

Nun ist gezeigt worden (vor. Kap. Nr. 7), daß, wenn die Zahlen

$$(2) \qquad \varrho_1, \varrho_2, \varrho_3, \ldots, \varrho_{p-1}$$

irgend ein reduziertes Restsystem (mod. p) bilden, z. B. das System der Zahlen $1, 2, 3, \ldots, p-1$, zu jeder Zahl ϱ dieses Systems eine andere Zahl ϱ' desselben gefunden werden kann von der Beschaffenheit, daß das Produkt $\varrho\varrho'$ einer beliebigen Zahl des Systems, etwa derjenigen, welche der gleichen Restklasse angehört wie a, kongruent und somit

$$(3) \qquad \varrho\varrho' \equiv a \pmod{p}$$

wird. Hier können ϱ, ϱ' nicht dieselbe Zahl des Systems (2) bezeichnen, wenn a quadratischer Nichtrest ist, da sonst im Gegenteil $\varrho^2 \equiv a$ (mod. p), die Kongruenz (1) also auflösbar wäre. Da nun auch zu einer bestimmten Zahl ϱ stets nur

eine einzige Zahl ϱ' des Systems (2) gehört, für welche $\varrho\varrho' \equiv a$ wird, weil die Kongruenz ersten Grades $\varrho x \equiv a$ (mod. p) nur eine Wurzel haben kann, so kann man, wenn a quadratischer Nichtrest ist, die $p-1$ Zahlen (2) in $\frac{p-1}{2}$ verschiedene Paare von Zahlen ϱ, ϱ' verteilen, deren Produkt jedesmal mit a kongruent wird. Multipliziert man alle diese Paare von Zahlen miteinander, so wird das entstehende Produkt einerseits das Produkt aller $p-1$ Zahlen (2), andererseits mit $a^{\frac{p-1}{2}}$ kongruent, also

$$\varrho_1\varrho_2\cdots\varrho_{p-1} \equiv a^{\frac{p-1}{2}} \pmod{p} \tag{4}$$

sein.

Ist dagegen a quadratischer Rest (mod. p), also eine Lösung der Kongruenz (1) vorhanden, die, wie schon bemerkt, durch p nicht teilbar sein kann, so gibt es auch im reduzierten Restsystem (2) eine Zahl ϱ so beschaffen, daß

$$\varrho^2 \equiv a \pmod{p},$$

und dann noch eine zweite, davon verschiedene Zahl $\varrho' \equiv -\varrho$ desselben, für welche ebenfalls $\varrho'^2 \equiv a$ (mod. p) ist. Sondert man das Paar dieser beiden Zahlen des Systems (2) ab, die ein Produkt $\varrho\varrho' \equiv -\varrho^2 \equiv -a$ geben, so werden die übrigen $p-3$ Zahlen des Systems wieder wie vorher so in $\frac{p-3}{2}$ Paare verteilt werden können, daß das Produkt der Zahlen jedes Paares kongruent a (mod. p) wird. Durch Multiplikation aller Paare miteinander erhält man daher einerseits wieder das Produkt aller $p-1$ Zahlen (2), das andererseits aber jetzt der Potenz $-a^{\frac{p-1}{2}}$ kongruent ist, und somit die Kongruenz

$$\varrho_1\varrho_2\cdots\varrho_{p-1} \equiv -a^{\frac{p-1}{2}} \pmod{p}. \tag{5}$$

Je nachdem also a quadratischer Rest oder Nichtrest ist (mod. p), findet die Kongruenz (5) oder die Kongruenz (4) statt. Nun ist gewiß $a = 1$ ein quadratischer Rest, da

$$x^2 \equiv 1 \pmod{p}$$

die beiden inkongruenten Lösungen $x \equiv 1$, $x \equiv -1 \pmod{p}$ besitzt. Daher folgt aus (5) für $a = 1$, daß

(6) $$\varrho_1 \varrho_2 \cdots \varrho_{p-1} \equiv -1 \pmod{p}$$

ist. Infolge dieses Umstandes aber können die Kongruenzen (5) und (4) einfacher geschrieben werden, wie folgt:

(7) $$a^{\frac{p-1}{2}} \equiv 1, \quad a^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

Der zuvor erhaltene Satz läßt sich daher folgendermaßen aussprechen: Je nachdem a quadratischer Rest oder Nichtrest ist $(\text{mod.} p)$, findet die erste oder die zweite der Kongruenzen (7) statt. Da aber eine durch p nicht teilbare Zahl entweder quadratischer Rest oder Nichtrest sein, eine der beiden Kongruenzen (7) also notwendig stattfinden muß, darf man auch umgekehrt sagen: Je nachdem die erste oder die zweite Kongruenz (7) stattfindet, ist a quadratischer Rest oder Nichtrest $(\text{mod.} p)$. Somit haben wir ein Kriterium erlangt, um bestimmt zu entscheiden, ob dies oder jenes der Fall ist; man nennt es das *Euler*sche Kriterium, weil *Euler* es zuerst aufgestellt hat.

Noch zwei andere wichtige Folgerungen können wir ziehen. Einmal ergibt sich, da, wie bemerkt, eine der Kongruenzen (7) notwendig erfüllt ist, durch deren Quadrierung in beiden Fällen die gemeinsame Kongruenz

(8) $$a^{p-1} \equiv 1 \pmod{p},$$

die also für jede durch p nicht teilbare Zahl a stattfindet, d. h. ein neuer Beweis des *Fermat*schen Satzes. Andererseits ist die Kongruenz (6) für jedes reduzierte Restsystem $(\text{mod.} p)$ erhalten worden, gilt also auch für das besondere System $1, 2, 3, \ldots, p-1$ dieser Art, und es findet daher auch nachstehende Kongruenz statt:

(9) $$1 \cdot 2 \cdot 3 \ldots (p-1) \equiv -1 \pmod{p}.$$

Sie wird als *Wilson*scher Satz bezeichnet, der besonders dadurch interessant ist, daß er ein Charakteristikum für Primzahlen abgibt, insofern er nicht nur stets stattfindet, wenn p eine Primzahl ist, sondern auch nur in diesem Falle. In der Tat, wäre p zusammengesetzt und q ein Teiler von p, so fände sich dieser als eine Zahl $< p$ in der Reihe der Faktoren der linken Seite, die somit einen Teiler mit dem

Modul p gemeinsam hätte, welchen doch die rechte Seite offenbar nicht hat, was unmöglich ist.

2. Da die $p-1$ Zahlen eines reduzierten Restsystems, je nachdem sie quadratischer Rest oder Nichtrest sind, die eine oder die andere der Kongruenzen (7) erfüllen, deren jede höchstens so viel Wurzeln hat, als ihr Grad $\frac{p-1}{2}$ beträgt, so erkennt man, daß jede von ihnen genau $\frac{p-1}{2}$ Wurzeln hat, daß also $\frac{p-1}{2}$ inkongruente quadratische Reste und ebensoviel inkongruente quadratische Nichtreste (mod. p) vorhanden sind.

Zur Unterscheidung, ob eine Zahl a quadratischer Rest oder Nichtrest sei, hat *Legendre* ein sehr bequemes Symbol eingeführt. Mit ihm setzen wir

$$(10)\qquad \left(\frac{a}{p}\right) = +1 \quad \text{oder} \quad \left(\frac{a}{p}\right) = -1\,,$$

je nachdem die durch p nicht teilbar vorausgesetzte Zahl a quadratischer Rest oder Nichtrest von p ist. Die Einheit $\left(\frac{a}{p}\right)$ wird daher nach dem *Euler*schen Kriterium durch die Kongruenz

$$(10\text{a})\qquad a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$$

bestimmt sein, aus welcher sich auch die fundamentalen Eigenschaften des *Legendre*schen Symbols $\left(\frac{a}{p}\right)$ ergeben.

Offenbar ist zunächst

$$(11)\qquad \left(\frac{a'}{p}\right) = \left(\frac{a}{p}\right), \quad \text{wenn} \quad a' \equiv a \pmod{p};$$

denn für zwei kongruente Zahlen a', a sind auch die Potenzen $a'^{\frac{p-1}{2}}$, $a^{\frac{p-1}{2}}$ einander kongruent, also ist wegen

$$a'^{\frac{p-1}{2}} \equiv \left(\frac{a'}{p}\right), \quad a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)$$

auch $\left(\frac{a'}{p}\right) \equiv \left(\frac{a}{p}\right) \pmod{p}$; da hier aber rechts und links **Einheiten** stehen, deren Differenz, je nachdem sie gleichen oder verschiedenen Vorzeichens sind, Null oder ± 2, mithin nur dann durch p teilbar ist, wenn sie gleichen Vorzeichens sind, führt vorstehende **Kongruenz** zur **Gleichheit** beider Einheiten, d. i. zur Formel (11).

Ferner ist für irgend zwei durch p nicht teilbare Zahlen a, a'

$$\left(\frac{a\,a'}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{a'}{p}\right). \tag{12}$$

In der Tat bestehen nach dem *Euler*schen Kriterium die Formeln

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right), \quad a'^{\frac{p-1}{2}} \equiv \left(\frac{a'}{p}\right), \quad (a\,a')^{\frac{p-1}{2}} \equiv \left(\frac{a\,a'}{p}\right),$$

während die Multiplikation der beiden ersten

$$(a\,a')^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \cdot \left(\frac{a'}{p}\right)$$

liefert; demnach wäre jedenfalls

$$\left(\frac{a\,a'}{p}\right) \equiv \left(\frac{a}{p}\right) \cdot \left(\frac{a'}{p}\right) \pmod{p}$$

und aus dieser **Kongruenz** der Einheiten schließt man wie vorher ihre **Gleichheit**, d. h. die Formel (12).

Dieser Formel gemäß ist das Produkt zweier quadratischen Reste sowie das Produkt zweier quadratischen Nichtreste (mod. p) stets ein quadratischer Rest, dagegen das Produkt aus einem quadratischen Rest in einen quadratischen Nichtrest stets ein quadratischer Nichtrest. Daher wird ein Produkt aus beliebig vielen, durch p nicht teilbaren Faktoren ein quadratischer Rest oder Nichtrest sein, je nachdem die Anzahl derjenigen Faktoren, welche Nichtreste sind, gerade oder ungerade ist.

Um hiervon eine interessante Anwendung zu machen, wählen wir als reduziertes Restsystem (mod. p) dasjenige, welches aus dem Systeme der absolut kleinsten Reste (mod. p)

durch Unterdrückung der Zahl Null entsteht, nämlich das System der Zahlen

$$(13)\qquad -\frac{p-1}{2}, -\frac{p-3}{2}, \ldots, -2, -1, 1, 2, \ldots, \frac{p-3}{2}, \frac{p-1}{2}.$$

So gewinnen wir an Stelle des *Wilson*schen Satzes aus der allgemeinen Kongruenz (6) die folgende:

$$(14)\qquad \left(1\cdot 2\cdot 3 \ldots \frac{p-1}{2}\right)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}.$$

Falls daher die Primzahl p von der Form $4k-1$, also $\frac{p+1}{2} = 2k$ ist, ist die Differenz beider Seiten voriger Kongruenz als Differenz zweier Quadrate zerlegbar in das Produkt der zwei Faktoren

$$1\cdot 2\cdot 3 \ldots \frac{p-1}{2} - (-1)^{\frac{p+1}{4}}$$

$$1\cdot 2\cdot 3 \ldots \frac{p-1}{2} + (-1)^{\frac{p+1}{4}},$$

von denen daher einer und, da ihre Differenz gleich ± 2, offenbar auch nur einer durch p teilbar sein wird, so daß, unter ε eine Einheit verstanden,

$$(15)\qquad 1\cdot 2\cdot 3 \ldots \frac{p-1}{2} \equiv \varepsilon \pmod{p}$$

gesetzt werden kann. Zur Entscheidung über das Vorzeichen bemerke man die nach (11) hieraus folgende Gleichung

$$\left(\frac{1\cdot 2\cdot 3 \ldots \frac{p-1}{2}}{p}\right) = \left(\frac{\varepsilon}{p}\right).$$

Heißt N die Anzahl der Nichtreste unter den Zahlen $1, 2, 3, \ldots, \frac{p-1}{2}$, so ist die linke Seite derselben dem letztausgesprochenen Satze gemäß gleich $(-1)^N$, während $\left(\frac{\varepsilon}{p}\right)$, falls $\varepsilon = 1$ ist, den Wert 1, und falls $\varepsilon = -1$ ist, für Primzahlen p von der gedachten Form $4k-1$, wie bald gezeigt werden wird (Nr. 4), den Wert -1 hat. Daraus ist zu

schließen, daß ε gleich $+1$ oder -1 zu setzen ist, je nachdem N gerade oder ungerade ist. Die Kongruenz (15) nimmt also nachstehende Gestalt an:

$$1 \cdot 2 \cdot 3 \ldots \frac{p-1}{2} \equiv (-1)^N \pmod{p} \tag{16}$$

und lehrt den **Satz:**

Ist p eine Primzahl von der Form $4k-1$, so ist das Produkt der Zahlen $1, 2, 3, \ldots, \frac{p-1}{2}$ der positiven oder negativen Einheit (mod. p) kongruent, je nachdem die Anzahl dieser Zahlen, welche quadratische Nichtreste (mod. p) sind, gerade oder ungerade ist.

3. Bedeutet a wieder eine durch p nicht teilbare Zahl, so werden nach Nr. 1 die Produkte aus a in die Zahlen (13) ein reduziertes Restsystem (mod. p) bilden, also, von der Reihenfolge abgesehen, diesen Zahlen kongruent sein. Daher werden, wenn wir nur die eine Hälfte dieser Produkte, nämlich die Produkte

$$1 \cdot a,\ 2 \cdot a,\ 3 \cdot a, \ldots, \frac{p-1}{2} \cdot a \tag{17}$$

in Betracht ziehen, auch sie $\frac{p-1}{2}$ verschiedenen Zahlen der Reihe (13) kongruent sein, unter denen eine Anzahl λ positiv sein, also der Reihe $1, 2, \ldots, \frac{p-1}{2}$ angehören, die übrigen $\mu = \frac{p-1}{2} - \lambda$ negativ, also der Reihe $-1, -2, \ldots, -\frac{p-1}{2}$ angehörig sein mögen. Nennen wir $\alpha_1, \alpha_2, \ldots, \alpha_\lambda$ die ersteren, $-\beta_1, -\beta_2, \ldots, -\beta_\mu$ die letzteren Reste, so ist offenbar das Produkt der Zahlen (17)

$$1 \cdot 2 \cdot 3 \ldots \frac{p-1}{2} \cdot a^{\frac{p-1}{2}} \equiv \alpha_1 \alpha_2 \ldots \alpha_\lambda \cdot (-1)^\mu \beta_1 \beta_2 \ldots \beta_\mu \pmod{p}. \tag{18}$$

Aber die $\frac{p-1}{2}$ Zahlen $\alpha_1, \alpha_2, \ldots, \alpha_\lambda, \beta_1, \beta_2, \ldots, \beta_\mu$ erfüllen die ganze Reihe der Zahlen $1, 2, 3, \ldots, \frac{p-1}{2}$,

denn sie gehören sämtlich dieser Reihe an und sind, wie leicht zu sehen, verschieden voneinander; in der Tat, da die Produkte (17) inkongruent sind, können keine zwei ihrer Reste α_i, α_k, auch keine zwei ihrer Reste $-\beta_i$, $-\beta_k$, also auch nicht β_i, β_k gleich sein, endlich aber kann auch kein α_i einem β_k gleich sein, da sonst $\alpha_i - \beta_k = 0$, also die Summe der entsprechenden Produkte (17) kongruent Null, d. i. durch p teilbar sein müßte, was offenbar nicht der Fall ist, da es a nicht ist, und die Summe zweier der Faktoren $1, 2, 3, \ldots, \frac{p-1}{2}$ kleiner ist als p. Hiernach ist

$$\alpha_1 \alpha_2 \ldots \alpha_\lambda \beta_1 \beta_2 \ldots \beta_\mu = 1 \cdot 2 \cdot 3 \ldots \frac{p-1}{2},$$

und da man mit diesem zu p teilerfremden Produkte die Kongruenz (18) heben darf, erhält man mit Rücksicht auf (10a) endlich die Kongruenz

$$\left(\frac{a}{p}\right) \equiv (-1)^\mu \pmod{p},$$

also die wichtige Gleichung

$$(19) \qquad \left(\frac{a}{p}\right) = (-1)^\mu .$$

Sie spricht folgenden **Satz** aus, der als *Gaußsches Lemma* bezeichnet zu werden pflegt:

Bedeutet μ die Anzahl der absolut kleinsten Reste der Vielfachen (17), welche negativ sind, so ist a quadratischer Rest oder Nichtrest von p, je nachdem μ gerade oder ungerade ist.

Beispiel: Sei $p = 19$ also $\frac{p-1}{2} = 9$, und $a = 7$; für die Vielfachen

$$1 \cdot 7, \quad 2 \cdot 7, \quad 3 \cdot 7, \quad 4 \cdot 7, \quad 5 \cdot 7, \quad 6 \cdot 7, \quad 7 \cdot 7, \quad 8 \cdot 7, \quad 9 \cdot 7$$

finden sich als absolut kleinste Reste (mod. 19) die Zahlen

$$7, \quad -5, \quad 2, \quad 9, \quad -3, \quad 4, \quad -8, \quad -1, \quad 6,$$

welche in der Tat, vom Vorzeichen abgesehen, die ganze Reihe 1, 2, 3, 4, 5, 6, 7, 8, 9 erfüllen; unter ihnen sind $\lambda = 5$ positiv und $\mu = 4$ negativ; da also μ gerade ist, muß 7 quadratischer Rest von 19 sein. Dies läßt sich

leicht bestätigen. Um nämlich für eine Primzahl p alle inkongruenten quadratischen Reste zu finden, genügt es offenbar, die Reste der Quadrate

$$1^2,\ 2^2,\ 3^2, \ldots (p-1)^2$$

(mod. p) zu ermitteln; es genügt sogar, dies für die Quadrate

$$1^2,\ 2^2,\ 3^2, \ldots \left(\frac{p-1}{2}\right)^2$$

zu tun, denn je zwei Quadrate

$$\alpha^2 \quad \text{und} \quad (p-\alpha)^2 = p^2 - 2p\alpha + \alpha^2$$

sind (mod. p) kongruent und geben also den gleichen quadratischen Rest. Führt man dies für $p = 19$ aus, so finden sich als Reste der Quadrate

$$1^2,\ 2^2,\ 3^2,\ 4^2,\ 5^2,\ 6^2,\ 7^2,\ 8^2,\ 9^2$$

die Zahlen

$$1,\ 4,\ 9,\ 16,\ 6,\ 17,\ 11,\ 7,\ 5,$$

und unter ihnen die Zahl 7.

4. Indem wir jetzt das *Gauß*sche Lemma an Stelle des *Euler*schen Kriteriums zur Grundlage nehmen, werden wir eine Reihe sehr eleganter Sätze ableiten können, mit deren Hilfe der quadratische Charakter einer Zahl in bezug auf den Modul p leicht bestimmbar ist.

Da nach Formel (11) kongruente Zahlen gleichen quadratischen Charakter haben, d. h. gleichzeitig quadratische Reste oder gleichzeitig quadratische Nichtreste sind, dürfte man sich auf die Zahlen beschränken, welche der Reihe $1, 2, 3, \ldots, p-1$ angehören, also positiv sind. Es ist aber bequemer, den Wert des Symbols $\left(\frac{a}{p}\right)$ wenigstens für die eine negative Zahl $a = -1$ beizubehalten, das an Stelle des Symbols $\left(\frac{p-1}{p}\right)$ gesetzt werden darf, wodurch dann nach der Formel

$$\left(\frac{-a}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{a}{p}\right)$$

das Symbol, falls es für alle positiven Zahlen ermittelt ist, auch für alle negativen Zahlen bestimmt sein wird.

Nach der Formel (12) leuchtet ferner ein, daß die Frage, ob eine gegebene Zahl a (mod. p) quadratischer Rest oder Nichtrest ist, aus dem bezüglichen Verhalten ihrer Faktoren entschieden werden kann. Man braucht daher nur den Fall zu erörtern, daß a eine Primzahl ist, d. h., wenn unter q irgend eine von p verschiedene ungerade Primzahl verstanden wird, die Fälle

$$a = 2, \quad a = q.$$

Es bleibt mithin der Wert der drei Symbole

$$\left(\frac{-1}{p}\right), \quad \left(\frac{2}{p}\right), \quad \left(\frac{q}{p}\right)$$

zu ermitteln.

Nun ergibt sich der Wert des Symbols $\left(\frac{-1}{p}\right)$ unmittelbar aus dem *Euler*schen Kriterium oder der Formel (10a), derzufolge die Kongruenz

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p},$$

also auch wieder die Gleichung

$$(20) \qquad \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

besteht. Da die ungerade Primzahl p durch 4 geteilt einen der Reste 1 oder 3 läßt und je nach diesen beiden Fällen $\frac{p-1}{2}$ gerade oder ungerade ist, so spricht die Formel (20) sich in folgendem **Satze** aus:

Die Zahl -1 ist quadratischer Rest von jeder Primzahl p von der Form $4k+1$ und quadratischer Nichtrest von jeder Primzahl p von der Form $4k+3$.

Fast ebenso einfach findet sich der Wert des Symbols $\left(\frac{2}{p}\right)$ mit Hilfe des Lemma von *Gauß*. Bezieht man dies Lemma auf die Zahl $a = 2$, so bedeutet μ die Anzahl der Vielfachen

$$(21) \qquad 1 \cdot 2, \ 2 \cdot 2, \ 3 \cdot 2, \ \ldots, \ \frac{p-1}{2} \cdot 2,$$

deren absolut kleinste Reste (mod. p) negativ sind. Diese Vielfachen sind die geraden Zahlen der Reihe

$$1, 2, 3, \ldots, p-1,$$

und von den letzteren geben offenbar diejenigen, welche $< \frac{p}{2}$ sind, positive, dagegen diejenigen, welche $> \frac{p}{2}$ sind, negative absolut kleinste Reste (mod. p). Es handelt sich daher nur darum, festzustellen, wieviel der Vielfachen (21) größer als $\frac{p}{2}$ sind. Nun ist $2 \cdot h > \frac{p}{2}$, wenn $h > \frac{p}{4}$ ist. Ist daher zuerst p von der Form $4k+1$, so werden die $k = \frac{p-1}{4}$ Vielfachen

$$(k+1) \cdot 2, \quad (k+2) \cdot 2, \quad \ldots, \quad 2k \cdot 2 = \frac{p-1}{2} \cdot 2$$

der Reihe (21) diejenigen sein, denen negative absolut kleinste Reste zukommen, und man erhält dann also

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{4}}. \tag{22a}$$

Wenn dagegen p von der Form $4k+3$ ist, so sind die $k+1 = \frac{p+1}{4}$ Vielfachen

$$(k+1) \cdot 2, \quad (k+2) \cdot 2, \quad \ldots, \quad (2k+1) \cdot 2 = \frac{p-1}{2} \cdot 2$$

diejenigen Vielfachen der Reihe (21), denen negative absolut kleinste Reste zukommen, und folglich ergibt sich dann

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p+1}{4}}. \tag{22b}$$

Die Primzahlen der ersteren Art zerfallen, je nachdem k gerade, gleich $2h$, oder ungerade, gleich $2h+1$ ist, in solche von der Form $8h+1$ und solche von der Form $8h+5$, und ihnen entsprechend ist $\frac{p-1}{4}$ resp. gerade oder ungerade; desgleichen zerfallen die Primzahlen der zweiten Art, je nachdem $k = 2h$ oder $k = 2h+1$ ist, in

solche von der Form $8h+3$ und solche von der Form $8h+7$, und ihnen entsprechend wird $\frac{p+1}{4}$ resp. ungerade oder gerade sein. Zufolge der erhaltenen Gleichungen (22a), (22b) wird daher $\left(\frac{2}{p}\right)=+1$, wenn $p=8h+1$ oder $8h+7$, dagegen $\left(\frac{2}{p}\right)=-1$, wenn $p=8h+3$ oder $8h+5$ ist. Man hat auf solche Weise folgenden

Satz: Die Zahl 2 ist quadratischer Rest von allen Primzahlen p von einer der beiden Formen $8h+1$, $8h+7$, dagegen quadratischer Nichtrest von allen Primzahlen von einer der beiden Formen $8h+3$, $8h+5$.

Nun findet man

$$\frac{(8h+1)^2-1}{8}=8h^2+2h$$

$$\frac{(8h+7)^2-1}{8}=8h^2+14h+6$$

$$\frac{(8h+3)^2-1}{8}=8h^2+6h+1$$

$$\frac{(8h+5)^2-1}{8}=8h^2+10h+3\,,$$

d. h. $\frac{p^2-1}{8}$ ist für die Primzahlen p der beiden ersten Formen eine gerade, für die Primzahlen der beiden zweiten Formen eine ungerade Zahl. Daher läßt sich der erhaltene Satz wieder in sehr einfacher Weise durch die Formel

(22) $$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$$

zum Ausdrucke bringen.

5. Was endlich die Bestimmung des dritten Symbols $\left(\frac{q}{p}\right)$ betrifft, so gilt hier ein Satz, der wegen seines eigentümlichen Charakters, insofern er den Wert des Symbols $\left(\frac{q}{p}\right)$ auf den des „reziproken" Symbols $\left(\frac{p}{q}\right)$ zurück-

führt, das Reziprozitätsgesetz der quadratischen Reste genannt wird. Zuerst von *Euler* in seinem vollen Umfange ausgesprochen, erhielt es durch *Legendre*, der auch einen ersten, doch unvollständigen Beweis desselben lieferte, seinen Namen sowie mittels des *Legendre*schen Symbols seinen hocheleganten Ausdruck. *Gauß* gab dann den ersten strengen Beweis des Gesetzes und ließ ihm noch sechs andere auf sehr verschiedenen Grundlagen beruhende Beweise folgen; von ihnen sind drei elementarer Natur und zwei unter diesen auf das *Gauß*sche Lemma begründet. Seitdem ist eine große Menge anderer Beweise dieses durch seine Schönheit wie seine Wichtigkeit gleich ausgezeichneten Satzes gegeben worden, deren Anzahl bereits größer als fünfzig ist*). Die überwiegende Mehrzahl derselben hat elementaren Charakter und zumeist das *Gauß*sche Lemma zum Ausgangspunkte. Hier müssen wir uns damit begnügen, einen einzigen dieser Beweise zur Dartellung zu bringen, und wir wählen dazu den dritten der von *Lange* (Leipz., Berichte der sächs. Ges. d. Wiss. 49, 1897, S. 607) gegebenen, der weiter keiner Vorbereitungen bedarf als einer leichten Umformung des *Gauß*schen Lemma, die an sich Interesse darbietet, und auch im übrigen von größter Ursprünglichkeit ist.

Zuvörderst soll gezeigt werden, daß der Exponent μ im *Gauß*schen Lemma, welcher, wenn es sich um das Symbol $\left(\frac{q}{p}\right)$ handelt, die Anzahl der Vielfachen

$$1 \cdot q,\ 2 \cdot q,\ 3 \cdot q,\ \ldots,\ \frac{p-1}{2} \cdot q \tag{23}$$

bezeichnet, deren absolut kleinste Reste (mod. p)

---

*) Der Leser, welcher genauer über die Beweise des Reziprozitätsgesetzes unterrichtet sein will, sei auf des Verf. „Niedere Zahlentheorie“ I, S. 203 sqq., verwiesen, wo eine systematische Darstellung derselben und ihres Verhältnisses zueinander sich findet. Die dort gegebene chronologische Tabelle der vorhandenen Beweise ist noch nicht ganz vollständig, es fehlen darin ein Beweis von *Kronecker* (Berl. Sitzgsber. Akad. 1880, S. 404), vier Beweise von *A. Tafelmacher* (Dissert. Göttingen 1889), ein Beweis von *Pepin* (Acad. Rom. P. N. Lincei 43, 1890, S. 192), von *Lerch* (J. sci. math. e astr. Teixeira, 1904, 15, S. 97) und von *T. Takagi* (reports of the meetings of the Tokyo Phys. Math. Soc. 1904). Ferner zwei Beweise von *Pellet*, C. R. Ac. Paris 87, 1878, S. 1071; Bull. Soc. math. France 17 (1888/9), S. 161.

negativ sind, noch eine andere Bedeutung hat. Denkt man sich nämlich nicht die absolut kleinsten, sondern die kleinsten positiven Reste (mod. p) jener Vielfachen bestimmt, indem man die Gleichungen aufstellt

$$(24) \qquad h \cdot q = a_h \cdot p + r_h$$
$$\left(\text{für} \quad h = 1, 2, 3, \ldots, \frac{p-1}{2}\right),$$

wo $0 < r_h < p$ gedacht ist, so bezeichnet μ auch die Anzahl der Fälle, in denen in diesen Gleichungen der Quotient a_h ungerade ausfällt.

In der Tat, ist a_h ungerade, so müssen hq und r_h und folglich auch die Zahlen h und r_h ungleichartig, die eine gerade, die andere ungerade sein. Ist nun zuerst h gerade, $h = 2h'$, wo also $h' < \frac{p}{4}$ ist, so läßt sich die Gleichung (24) schreiben, wie folgt:

$$2h' \cdot q = (a_h + 1) \cdot p - (p - r_h)$$

und gibt

$$h' \cdot q = \frac{a_h + 1}{2} \cdot p - \frac{p - r_h}{2},$$

wo $\frac{p - r_h}{2} < \frac{p}{2}$; also entspricht jeder der Gleichungen (24) mit ungeradem Quotienten und geradem h ein Vielfaches $h'q$ der Reihe (23), bei welchem $h' < \frac{p}{4}$ ist, mit negativem absolut kleinsten Reste, und wegen $h = 2h'$ entsprechen verschiedenen Gleichungen jener Art auch verschiedene Vielfache dieser Art. Ist aber h ungerade, so liefert die Gleichung (24), in welcher nun r_h gerade ist, die folgende:

$$(p - h) \cdot q = (q - a_h) \cdot p - r_h,$$

und weiter, wenn $p - h = 2h''$ gesetzt wird, wo jetzt $\frac{p}{4} < h'' < \frac{p}{2}$ ist,

$$h'' \cdot q = \frac{q - a_h}{2} \cdot p - \frac{r_h}{2},$$

wo $\frac{r_h}{2} < \frac{p}{2}$; also entspricht auch jeder der Gleichungen (24) mit ungeradem Quotienten und ungeradem h ein Viel-

faches $h''q$ der Reihe (23) mit negativem absolut kleinsten Reste, und es entsprechen verschiedenen jener Gleichungen auch verschiedene dieser Vielfachen; auch sind die letzteren, da $h'' > \frac{p}{4}$, von den früheren, bei denen $h' < \frac{p}{4}$ war, verschieden. Man schließt also, daß den sämtlichen Gleichungen (24) mit ungeradem Quotienten a_h ebensoviel verschiedene Vielfache der Reihe (23) mit negativem absolut kleinsten Reste entsprechen.

Aber auch umgekehrt. Ist

$$h'q = kp - r$$

ein Vielfaches mit negativem absolut kleinsten Reste und $h' < \frac{p}{4}$, so folgt

$$2h' \cdot q = (2k-1)p + (p-2r),$$

d. i. eine Gleichung der Reihe (24) mit ungeradem Quotienten und geradem Koeffizienten von q. Ist aber $h' > \frac{p}{4}$, so darf man schreiben

$$(p - 2h') \cdot q = (q - 2k) \cdot p + 2r,$$

wo $2r < p$, was also wieder eine Gleichung der Reihe (24) mit ungeradem Quotienten ist, welche von der vorigen verschieden ist, da in ihr der Koeffizient von q ungerade ist. Somit entsprechen also auch umgekehrt allen Vielfachen der Reihe (23) mit negativem absolut kleinsten Reste ebensoviel verschiedene Gleichungen der Reihe (24) mit ungeradem Quotienten. — Dies mit dem zuerst Festgestellten zusammen bestätigt die ausgesprochene Behauptung und gestattet also das *Gauß*sche Lemma in folgender Weise zu fassen:

Bedeutet μ die Anzahl der Fälle, in denen in den Gleichungen (24) der Quotient a_h ungerade ist, so ist

$$\left(\frac{q}{p}\right) = (-1)^{\mu}. \tag{25}$$

6. Stellt man nun neben den Gleichungen (24) auch die folgenden, analog gebildeten Gleichungen auf:

$$k \cdot p = b_k \cdot q + s_k \tag{26}$$

$$\left(\text{für} \quad k = 1, 2, 3, \ldots, \frac{q-1}{2}\right),$$

worin $0 < s_k < q$ gedacht ist, und bezeichnet mit ν die Anzahl der Fälle, in denen in diesen Gleichungen der Quotient b_k ungerade ist, so findet sich ebenso

$$(27) \qquad \left(\frac{p}{q}\right) = (-1)^{\nu}.$$

Da von den zwei verschiedenen Primzahlen p, q eine den größeren Wert haben muß, sei etwa $q > p$. Dann ist

$$h \cdot q \lesseqgtr \frac{p-1}{2} \cdot q \quad \text{d. i.} \quad \frac{q-1}{2} \cdot p - \frac{q-p}{2} < \frac{q-1}{2} \cdot p$$

und folglich jeder der Quotienten a_k in den Gleichungen (24) kleiner als $\frac{q-1}{2}$. Andererseits ist in den Gleichungen (26) jedenfalls $b_1 = 0$; da

$$\frac{q-1}{2} \cdot p = \frac{p-1}{2} \cdot q + \frac{q-p}{2} > \frac{p-1}{2} \cdot q$$

aber kleiner als $\frac{p+1}{2} \cdot q$ ist, so ist $b_{\frac{q-1}{2}} = \frac{p-1}{2}$; ferner folgt aus (26)

$$(k+1)\,p = b_k \cdot q + (p + s_k),$$

wo $p + s_k$ wegen $p < q$, $s_k < q$ den Wert $2q$ nicht erreicht; mithin ist b_{k+1} entweder gleich b_k oder um eine Einheit größer. Die Quotienten b_k in den Gleichungen (26) wachsen also von Null bis $\frac{p-1}{2}$, indem sie alle Zwischenwerte durchlaufen.

Dies vorausgeschickt, schreibe man die Gleichung (24) in der Form

$$(28) \qquad a_h \cdot p = (h-1)\,q + (q - r_h).$$

Da $r_h < p < q$ und, wie bemerkt, $a_h < \frac{q-1}{2}$ ist, so ist diese so umgeschriebene Gleichung (24) auch eine der Gleichungen (26). Die auf sie folgende der letzteren Gleichungen wird daher

$$(a_h + 1) \cdot p = h\,q + (p - r_h)$$

sein, also ist die Gleichung (28), welcher in der Reihe der Gleichungen (26) die $a_h$te Stelle zukommt, die letzte dieser

Gleichungen mit dem Quotienten $h-1$; ebenso würde die a_{h+1}te Gleichung (26) die letzte mit dem Quotienten h, und folglich die Anzahl dieser Gleichungen, denen der Quotient h zukommt, gleich $a_{h+1}-a_h$ sein. Der äußerste Wert, den man bei dieser Betrachtung dem Index h beilegen darf, ist $h=\frac{p-3}{2}$; die $a_{\frac{p-1}{2}}$te der Gleichungen (26) hätte noch den Quotienten $\frac{p-3}{2}$, während die folgende schon den Quotienten $\frac{p-1}{2}$ hätte, den nun, da auch der letzte Quotient $b_{\frac{q-1}{2}}$ noch gleich $\frac{p-1}{2}$ ist, wie gezeigt worden, alle Gleichungen (26) bis zur letzten, welcher die Stelle $\frac{q-1}{2}$ zukommt, beibehalten; die Anzahl der Gleichungen (26) mit dem Quotienten $\frac{p-1}{2}$ beträgt daher $\frac{q-1}{2}-a_{\frac{p-1}{2}}$.

Zählt man demnach die Gleichungen (26), denen ein ungerader Quotient 1, 3, 5, ... zukommt, so gibt es deren resp. a_2-a_1, a_4-a_3, a_6-a_5, ... Ihre Gesamtzahl ν bestimmt sich also, wenn $\frac{p-1}{2}$ gerade, also p von der Form $4k+1$ ist, durch die Gleichung

$$(29\text{a})\qquad \nu=-a_1+a_2-a_3+a_4-\ldots-a_{\frac{p-3}{2}}+a_{\frac{p-1}{2}},$$

dagegen, wenn $\frac{p-1}{2}$ ungerade, d. i. p von der Form $4k+3$ ist, durch die Gleichung

$$(29\text{b})\qquad \nu=-a_1+a_2-a_3+a_4-\ldots-a_{\frac{p-1}{2}}+\frac{q-1}{2}.$$

Faßt man aber diese Gleichungen als Kongruenzen (mod. 2), so kann man die erstere schreiben, wie folgt:

$$\nu\equiv a_1+a_2+a_3+a_4+\ldots+a_{\frac{p-3}{2}}+a_{\frac{p-1}{2}}\pmod{2},$$

woraus man nun, die geraden a_i unterdrückend und die ungeraden a_i, deren Anzahl μ genannt war, durch ihren Rest 1 ersetzend, sogleich

$$(30\text{a})\qquad \nu\equiv\mu\pmod{2}$$

erschließt. Ganz ebenso liefert die Gleichung (29b) die Kongruenz

$$\nu \equiv \mu + \frac{q-1}{2} \pmod{2}. \tag{30b}$$

Da nun Potenzen von -1, deren Exponenten nur um Vielfache von Zwei verschieden sind, gleichen Wert haben, folgt im ersten Falle, d. h. wenn p von der Form $4k+1$ ist, aus (27) in Verbindung mit (25) die Gleichung

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right),$$

im zweiten Falle aber, d. h. wenn p von der Form $4k+3$ ist,

$$\left(\frac{p}{q}\right) = (-1)^{\frac{q-1}{2}} \cdot \left(\frac{q}{p}\right),$$

mithin wieder $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$, wenn $\frac{q-1}{2}$ gerade, d. h. q von der Form $4k+1$ ist, und nur, wenn auch q von der Form $4k+3$ ist, $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.

Zusammenfassend kann man also das Gesetz aussprechen:

Wenn wenigstens eine der beiden Primzahlen p, q von der Form $4k+1$ ist, haben die beiden reziproken Symbole $\left(\frac{p}{q}\right), \left(\frac{q}{p}\right)$ gleichen, dagegen entgegengesetzten Wert, wenn beide Primzahlen von der Form $4k+3$ sind.

Bemerkt man schließlich, daß das Produkt $\frac{p-1}{2} \cdot \frac{q-1}{2}$ im ersten dieser beiden Fälle gerade, im letzten ungerade ist, daß also je nach diesen beiden Fällen

$$(-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} = +1 \quad \text{oder} \quad = -1$$

wird, so kann man das Gesetz auch durch die Formel

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \cdot \left(\frac{q}{p}\right)$$

oder, indem man mit $\left(\frac{q}{p}\right)$ multipliziert und beachtet, daß das Quadrat $\left(\frac{q}{p}\right)^2$ einer Einheit stets $+1$ ist, symmetrischer durch die folgende:

$$\left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \tag{31}$$

zum Ausdruck bringen.

Diese elegante Formel ist das Reziprozitätsgesetz der quadratischen Reste in der ihm von *Legendre* gegebenen Gestalt.

7. *Jacobi* hat eine Verallgemeinerung des *Legendre*schen Symbols eingeführt, welche gestattet, die für das letztere in den Formeln (20), (22) und (31) festgestellten Gesetze selbst zu verallgemeinern, indem man sie auf zusammengesetzte Zahlen ausdehnt.

Sei P irgend eine positive ungerade Zahl; wir setzen

$$P = pp'p'' \ldots, \tag{32}$$

indem wir unter $p, p', p'', \ldots$ die gleichen oder ungleichen Primfaktoren verstehen, in welche P sich zerlegen läßt. Ist dann a eine zu P teilerfremde Zahl, so soll das Symbol $\left(\frac{a}{P}\right)$ durch die Gleichung

$$\left(\frac{a}{P}\right) = \left(\frac{a}{p}\right)\cdot\left(\frac{a}{p'}\right)\cdot\left(\frac{a}{p''}\right)\ldots \tag{33}$$

definiert werden.

Es befolgt ganz gleiche fundamentale Gesetze, wie sie für das einfache *Legendre*sche Symbol in den Formeln (11) und (12) sich aussprechen. Sind nämlich a, a' zwei (mod. P) kongruente, zu P teilerfremde Zahlen, in Zeichen

$$a' \equiv a \pmod{P}, \tag{34}$$

so bestehen auch die Kongruenzen

$$a' \equiv a \pmod{p}, \quad a' \equiv a \pmod{p'}, \quad a' \equiv a \pmod{p''}, \ldots$$

und ihnen zufolge wegen (11) die Gleichungen

$$\left(\frac{a'}{p}\right) = \left(\frac{a}{p}\right), \quad \left(\frac{a'}{p'}\right) = \left(\frac{a}{p'}\right), \quad \left(\frac{a'}{p''}\right) = \left(\frac{a}{p''}\right), \ldots,$$

aus deren Multiplikation ineinander bei Beachtung der Definitionsgleichung (33) und der ihr entsprechenden Gleichung

$$\left(\frac{a'}{P}\right) = \left(\frac{a'}{p}\right) \cdot \left(\frac{a'}{p'}\right) \cdot \left(\frac{a'}{p''}\right) \cdots$$

die Formel

(35) $$\left(\frac{a'}{P}\right) = \left(\frac{a}{P}\right) \quad \text{für} \quad a' \equiv a \quad (\text{mod.}\, P)$$

hervorgeht; für zwei (mod. P) kongruente Werte a, a' hat also auch das *Jacobi*sche Symbol gleichen Wert.

Sind ferner a, a' irgend zwei zu P teilerfremde Zahlen, so gilt dasselbe auch von $a a'$, und folglich hat man zu setzen

$$\left(\frac{a a'}{P}\right) = \left(\frac{a a'}{p}\right) \cdot \left(\frac{a a'}{p'}\right) \cdot \left(\frac{a a'}{p''}\right) \cdots;$$

jedes der *Legendre*schen Symbole zur Rechten aber kann nach Formel (12) in das Produkt zweier anderen aufgelöst und somit

$$\left(\frac{a a'}{P}\right) = \left(\frac{a}{p}\right) \left(\frac{a}{p'}\right) \left(\frac{a}{p''}\right) \cdots \left(\frac{a'}{p}\right) \left(\frac{a'}{p'}\right) \left(\frac{a'}{p''}\right) \cdots,$$

d. h.

(36) $$\left(\frac{a a'}{P}\right) = \left(\frac{a}{P}\right) \cdot \left(\frac{a'}{P}\right)$$

geschrieben werden.

Zu diesen beiden Grundformeln (35), (36) tritt für das *Jacobi*sche Symbol noch eine dritte hinzu. Sei nämlich auch Q eine positive ungerade Zahl und

(37) $$Q = q q' q'' \cdots$$

ihre Zerlegung in Primfaktoren; dann wird, wenn a eine Zahl bedeutet, welche sowohl zu P als auch zu Q und daher auch zu ihrem Produkte

$$PQ = p p' p'' \cdots q q' q'' \cdots$$

teilerfremd ist,

$$\left(\frac{a}{P}\right) = \left(\frac{a}{p}\right) \left(\frac{a}{p'}\right) \left(\frac{a}{p''}\right) \cdots$$

$$\left(\frac{a}{Q}\right) = \left(\frac{a}{q}\right) \left(\frac{a}{q'}\right) \left(\frac{a}{q''}\right) \cdots$$

$$\left(\frac{a}{PQ}\right) = \left(\frac{a}{p}\right) \left(\frac{a}{p'}\right) \cdots \left(\frac{a}{q}\right) \left(\frac{a}{q'}\right) \cdots$$

und folglich

(38) $$\left(\frac{a}{PQ}\right) = \left(\frac{a}{P}\right) \cdot \left(\frac{a}{Q}\right)$$

sein.

Aus diesen Formeln ergibt sich nun zunächst

$$\left(\frac{-1}{P}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{-1}{p'}\right) \cdot \left(\frac{-1}{p''}\right) \ldots,$$

d. i. nach (20)

(39) $$\left(\frac{-1}{P}\right) = (-1)^{\frac{p-1}{2} + \frac{p'-1}{2} + \frac{p''-1}{2} + \cdots}$$

und ebenso

$$\left(\frac{2}{P}\right) = \left(\frac{2}{p}\right) \cdot \left(\frac{2}{p'}\right) \cdot \left(\frac{2}{p''}\right) \ldots,$$

d. i. nach (22)

(40) $$\left(\frac{2}{P}\right) = (-1)^{\frac{p^2-1}{8} + \frac{p'^2-1}{8} + \frac{p''^2-1}{8} + \cdots}$$

Schreibt man aber die Formel (32) wie folgt:

$$P = (1 + (p-1))(1 + (p'-1))(1 + (p''-1)) \ldots$$

und bedenkt, daß das Produkt von zwei oder mehreren der geraden Zahlen $p-1$, $p'-1$, $p''-1, \ldots$ durch 4 aufgeht, so liefert die Formel die Kongruenz

$$P - 1 \equiv (p-1) + (p'-1) + (p''-1) + \ldots \quad (\text{mod. } 4),$$

also

$$\frac{P-1}{2} \equiv \frac{p-1}{2} + \frac{p'-1}{2} + \frac{p''-1}{2} + \ldots \quad (\text{mod. } 2),$$

und die Gleichung (39) läßt sich folgendermaßen schreiben:

(41) $$\left(\frac{-1}{P}\right) = (-1)^{\frac{P-1}{2}}.$$

Ebenso ist

$$P^2 = (1 + (p^2-1))(1 + (p'^2-1))(1 + (p''^2-1)) \ldots$$

Da nun das Quadrat jeder ungeraden Zahl, d. i. jeder Zahl von einer der beiden Formen $4k \pm 1$, durch 8 geteilt den Rest 1 läßt, indem

$$(4k \pm 1)^2 = 16k^2 \pm 8k + 1$$

ist, so sind die Zahlen p^2-1, p'^2-1, $p''^2-1, \dots$ sämtlich durch 8, jedes Produkt von zwei oder mehreren derselben also durch 64 teilbar; man erhält daher aus der obigen Gleichung für P^2 die Kongruenz

$$P^2-1 \equiv (p^2-1)+(p'^2-1)+(p''^2-1)+\dots \pmod{64}$$

und daraus

$$\frac{P^2-1}{8} \equiv \frac{p^2-1}{8}+\frac{p'^2-1}{8}+\frac{p''^2-1}{8}+\dots \pmod{8},$$

also auch (mod. 2), und somit statt der Gleichung (40) die einfachere folgende:

$$(42) \qquad \left(\frac{2}{P}\right)=(-1)^{\frac{P^2-1}{8}}.$$

Hiernach gelten die Formeln (20) und (22) also auch dann, wenn der Nenner des Symbols eine beliebig zusammengesetzte positive ungerade Zahl ist.

Um auch das Reziprozitätsgesetz zu verallgemeinern, bilden wir das Produkt der beiden *Jacobi*schen Symbole

$$\left(\frac{P}{Q}\right)=\left(\frac{P}{q}\right)\left(\frac{P}{q'}\right)\left(\frac{P}{q''}\right)\dots$$

$$\left(\frac{Q}{P}\right)=\left(\frac{Q}{p}\right)\left(\frac{Q}{p'}\right)\left(\frac{Q}{p''}\right)\dots,$$

indem wir P, Q als teilerfremde ungerade positive Zahlen voraussetzen. Löst man hier die einzelnen *Legendre*schen Symbole nach Formel (12) weiter auf, so erhält man offenbar im Ausdrucke des Produktes $\left(\frac{P}{Q}\right)\cdot\left(\frac{Q}{P}\right)$ jedes der Symbole

$$\left(\frac{p}{q}\right),\ \left(\frac{p'}{q}\right),\ \dots,\ \left(\frac{p}{q'}\right),\ \left(\frac{p'}{q'}\right),\ \dots$$

mit jedem der Symbole

$$\left(\frac{q}{p}\right),\ \left(\frac{q}{p'}\right),\ \dots,\ \left(\frac{q'}{p}\right),\ \left(\frac{q'}{p'}\right),\ \dots$$

bzw. multipliziert, was kurz ausgedrückt werde durch die Formel

$$\left(\frac{P}{Q}\right)\cdot\left(\frac{Q}{P}\right)=\prod\left(\frac{p}{q}\right)\left(\frac{q}{p}\right).$$

Wird aber hier das allgemeine Glied unter dem Produktzeichen nach (31) durch $(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$ ersetzt, so nimmt vorstehende Formel die Gestalt an:

$$(43) \qquad \left(\frac{P}{Q}\right)\cdot\left(\frac{Q}{P}\right) = (-1)^{\sum\frac{p-1}{2}\cdot\frac{q-1}{2}},$$

wo nun der Exponent von -1 die Summe aller Zahlen von der Form $\frac{p-1}{2}\cdot\frac{q-1}{2}$ bedeutet, welche man erhält, wenn man jeden der Primfaktoren $p, p', p'', \ldots$ mit jedem der Primfaktoren $q, q', q'', \ldots$ kombiniert, eine Summe, welche dem Produkte

$$\left(\frac{p-1}{2}+\frac{p'-1}{2}+\ldots\right)\left(\frac{q-1}{2}+\frac{q'-1}{2}+\ldots\right)$$

gleich ist. Den ersten dieser beiden Faktoren fanden wir schon (mod. 2) mit $\frac{P-1}{2}$ kongruent, ganz ebenso ist es der zweite mit $\frac{Q-1}{2}$ und daher der Exponent in (43) mit $\frac{P-1}{2}\cdot\frac{Q-1}{2}$. So geht endlich die Formel (43) in die folgende:

$$(44) \qquad \left(\frac{P}{Q}\right)\cdot\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}$$

über und lehrt, daß auch das Reziprozitätsgesetz gültig bleibt, wenn die positiven ungeraden Zahlen, welche Zähler und Nenner der beiden reziproken Symbole bilden, nicht Primzahlen, sondern beliebig zusammengesetzt sind, vorausgesetzt nur, daß sie teilerfremd sind.

Man darf endlich sogar eine der beiden Zahlen P, Q als negativ annehmen, wenn man übereinkommt, unter dem Symbole $\left(\frac{P}{-Q}\right)$ dasselbe zu verstehen, wie unter dem Symbole $\left(\frac{P}{Q}\right)$. In der Tat ist dann

$$\left(\frac{P}{-Q}\right)\cdot\left(\frac{-Q}{P}\right) = \left(\frac{P}{Q}\right)\cdot\left(\frac{Q}{P}\right)\cdot\left(\frac{-1}{P}\right),$$

also nach (44) und (41)

$$\left(\frac{P}{-Q}\right)\cdot\left(\frac{-Q}{P}\right)=(-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}+\frac{P-1}{2}};$$

da aber der Exponent von -1 gleich

$$\frac{P-1}{2}\cdot\frac{Q+1}{2}\equiv\frac{P-1}{2}\cdot\frac{-Q-1}{2}\pmod{2}$$

ist, darf schließlich geschrieben werden

$$(45)\qquad \left(\frac{P}{-Q}\right)\cdot\left(\frac{-Q}{P}\right)=(-1)^{\frac{P-1}{2}\cdot\frac{-Q-1}{2}},$$

was bewiesen werden sollte.

8. Wir sind nun in der Lage, die in Nr. 4 gestellte Aufgabe zu lösen, nämlich den Wert der drei Symbole

$$\left(\frac{-1}{p}\right),\quad \left(\frac{2}{p}\right),\quad \left(\frac{q}{p}\right)$$

zu bestimmen. Die beiden ersten ergeben sich unmittelbar aus den Formeln (20) und (22), der Wert des dritten wird leicht gefunden, wenn man mit dem verallgemeinerten Reziprozitätsgesetze (45) den *Euklid*ischen Algorithmus verbindet. Auf diese Weise hat *Eisenstein* eine einfache Regel aufgestellt, die Bestimmung von $\left(\frac{p}{q}\right)$ und allgemeiner von $\left(\frac{P}{Q}\right)$ zu leisten, und ähnliche sind später von *Kronecker*, *Lebesgue*, *Sylvester*, *Gegenbauer* gegeben worden.*)

Setzt man, unter P, Q zwei ungerade teilerfremde Zahlen verstehend, von denen Q positiv ist, dem *Euklid*ischen Algorithmus gemäß

$$P=kQ+Q_1,$$

wo Q_1 positiv und kleiner als Q gedacht ist, so kann statt dessen auch

$$P=(k+1)Q-(Q-Q_1)$$

*) *Eisenstein*, Journ. f. Math. von *Crelle*, 27, 1844, S. 317; *Kronecker*, Berl. Akad. Sitzungsber. 1884, S. 519; 1880, S. 698; *Sylvester*, Paris. C. Rendus 90, 1880, S. 1053; *Gegenbauer*, Wien. Ak. Berichte, 82 II, 1880, S. 931; 84 II, 1881, S. 1089.

geschrieben werden, während der Rest $-(Q-Q_1)$ wieder numerisch kleiner als Q, jetzt aber negativ ist; einer der beiden Quotienten k, $k+1$ aber muß eine gerade Zahl sein. Man kann also den *Euklid*ischen Algorithmus stets so einrichten, daß der Quotient jeder der Divisionen gerade ausfällt, und schreiben

$$P = 2h \cdot Q + \varepsilon_1 Q_1,$$

wo Q_1 wieder positiv und kleiner als Q zu denken und ε_1 gleich $+1$ oder -1 ist, und erhält ebenso fortfahrend den *Euklid*ischen Algorithmus in der folgenden Gestalt:

$$(46)\qquad \left\{\begin{array}{l} P = 2h \cdot Q + \varepsilon_1 Q_1 \\ Q = 2h_1 \cdot Q_1 + \varepsilon_2 Q_2 \\ Q_1 = 2h_2 \cdot Q_2 + \varepsilon_3 Q_3 \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ Q_{k-1} = 2h_k \cdot Q_k + \varepsilon_{k+1} Q_{k+1}, \end{array}\right.$$

wo die Zeichen $\varepsilon_1, \varepsilon_2, \varepsilon_3, \ldots, \varepsilon_{k+1}$ positive oder negative Einheiten bedeuten, je zwei aufeinanderfolgende Reste Q_i, Q_{i+1} teilerfremd und zuletzt einer der Reste, etwa Q_{k+1}, gleich 1 sein muß, da P, Q ohne gemeinsamen Teiler vorausgesetzt sind. Aus der allgemeinen Gleichung

$$(47)\qquad Q_{i-1} = 2h_i \cdot Q_i + \varepsilon_{i+1} Q_{i+1}$$

dieses Schemas folgt aber die Kongruenz

$$Q_{i-1} \equiv \varepsilon_{i+1} Q_{i+1} \pmod{Q_i},$$

also

$$\left(\frac{Q_{i-1}}{Q_i}\right) = \left(\frac{\varepsilon_{i+1} Q_{i+1}}{Q_i}\right);$$

dem verallgemeinerten Reziprozitätsgesetze (45) gemäß darf man hierfür setzen

$$\left(\frac{Q_{i-1}}{Q_i}\right) = \left(\frac{Q_i}{Q_{i+1}}\right) \cdot (-1)^{\frac{Q_i - 1}{2} \cdot \frac{\varepsilon_{i+1} Q_{i+1} - 1}{2}}.$$

Man bilde diese Gleichung für $i = 1, 2, 3, \ldots, k$, so entstehen k Gleichungen, deren letzte wegen $Q_{k+1} = 1$ so lautet:

$$\left(\frac{Q_{k-1}}{Q_k}\right) = \left(\frac{\varepsilon_{k+1}}{Q_k}\right),$$

oder in die Gestalt

$$\left(\frac{Q_{k-1}}{Q_k}\right) = (-1)^{\frac{Q_k-1}{2}\cdot\frac{\varepsilon_{k+1}Q_{k+1}-1}{2}}$$

gesetzt werden kann, denn diese Potenz ist in der Tat gleich 1 oder gleich $(-1)^{\frac{Q_k-1}{2}}$, je nachdem $\varepsilon_{k+1} = +1$ oder -1 ist. Fügt man diesen Gleichungen noch die aus der ersten Gleichung des Schemas (46) auf gleiche Weise gewonnene

$$\left(\frac{P}{Q}\right) = \left(\frac{Q}{Q_1}\right)\cdot(-1)^{\frac{Q-1}{2}\cdot\frac{\varepsilon_1 Q_1-1}{2}}$$

hinzu, so liefert deren Multiplikation ineinander, wie sogleich zu übersehen, die neue Gleichung

$$(48) \qquad \left(\frac{P}{Q}\right) = (-1)^{\sum\limits_{i=0}^{k}\frac{Q_i-1}{2}\cdot\frac{\varepsilon_{i+1}Q_{i+1}-1}{2}}.$$

Im Exponenten dieser Potenz von -1, welcher die Summe aller Zahlen von der Form

$$(49) \qquad \frac{Q_i-1}{2}\cdot\frac{\varepsilon_{i+1}Q_{i+1}-1}{2}$$

für die Werte $i = 0, 1, 2, \ldots, k$ bedeutet, dürfen aber die geraden Summanden unterdrückt und die ungeraden durch ihren Rest 1 (mod. 2) ersetzt werden; geschieht dies, so bezeichnet der neue Exponent die Anzahl der Fälle, wo der allgemeine Summand (49) ungerade, d. h. die Anzahl der Fälle, wo in den einzelnen Gleichungen (47) gleichzeitig Q_i und $\varepsilon_{i+1}Q_{i+1}$ von der Form $4k+3$ sind. Die Formel (48) lehrt also folgende

Regel: Man zähle, wie oft in den einzelnen Gleichungen des Schemas (46) die darin auftretenden Zahlen Q_i und $\varepsilon_{i+1}Q_{i+1}$ gleichzeitig von der Form $4k+3$ sind; ist N diese Anzahl, so ist

$$(50) \qquad \left(\frac{P}{Q}\right) = (-1)^N.$$

Beispiele: 1. Die Zahlen $p = 743$, $q = 211$ sind Primzahlen; man sucht den Wert des Symbols $\left(\frac{743}{211}\right)$. Das Schema (46) nimmt die Gestalt an

$$
\begin{aligned}
743 &= 4 \cdot 211 - 101 \; * \\
211 &= 2 \cdot 101 + 9 \\
101 &= 12 \cdot 9 - 7 \\
9 &= 2 \cdot 7 - 5 \; * \\
7 &= 2 \cdot 5 - 3 \\
5 &= 2 \cdot 3 - 1 \; *;
\end{aligned}
$$

in diesen Gleichungen bieten die mit einem Sternchen versehenen den Fall zweier Zahlen von der Form $4k + 3$, daher ist $N = 3$ und $\left(\frac{743}{211}\right) = -1$. Man bestätigt dies durch folgende Betrachtung: Nach (11) ist $\left(\frac{743}{211}\right) = \left(\frac{110}{211}\right)$, was wegen (12) gleich $\left(\frac{5}{211}\right) \cdot \left(\frac{2}{211}\right) \cdot \left(\frac{11}{211}\right)$ gesetzt werden kann; der zweite Faktor ist nach (22) gleich -1, die anderen nach dem Reziprozitätsgesetze gleich $\left(\frac{211}{5}\right) = \left(\frac{1}{5}\right) = 1$ resp. $-\left(\frac{211}{11}\right) = -\left(\frac{2}{11}\right) = +1$; im ganzen also wird $\left(\frac{743}{211}\right)$ gleich -1. Die Primzahl 743 ist also quadratischer Nichtrest der Primzahl 211.

2. Da die *Eisenstein*sche Regel auch für zusammengesetzte Zahlen gilt, nehme man z. B. $P = -1365$, $Q = 5428681$. Das Schema (46) wird hier das folgende:

$$
\begin{aligned}
1365 &= 0 \cdot Q + 1365 \\
Q &= 3978 \cdot 1365 - 1289 \\
1365 &= 2 \cdot 1289 - 1213 \\
1289 &= 2 \cdot 1213 - 1137 \\
1213 &= 2 \cdot 1137 - 1061 \\
1137 &= 2 \cdot 1061 - 985 \\
1061 &= 2 \cdot 985 - 909
\end{aligned}
$$

$$\begin{aligned}
985 &= 2\cdot 909 - 833\\
909 &= 2\cdot 833 - 757\\
833 &= 2\cdot 757 - 681\\
757 &= 2\cdot 681 - 605\\
681 &= 2\cdot 605 - 529\\
605 &= 2\cdot 529 - 453\\
529 &= 2\cdot 453 - 377\\
453 &= 2\cdot 377 - 301\\
377 &= 2\cdot 301 - 225\\
301 &= 2\cdot 225 - 149\\
225 &= 2\cdot 149 - 73\\
149 &= 2\cdot 73 + 3\\
73 &= 24\cdot 3 + 1\,.
\end{aligned}$$

Keine dieser Gleichungen bietet den Fall zweier Zahlen von der Form $4k+3$, daher ist $N=0$ und $\left(\frac{1365}{Q}\right)=+1$. Daraus folgt auch

$$\left(\frac{-1365}{Q}\right)=\left(\frac{-1}{Q}\right)\cdot\left(\frac{1365}{Q}\right)=+1\,,$$

da $Q\equiv 1 \pmod{4}$, also $\left(\frac{-1}{Q}\right)=1$ ist. Dies bestätigt sich wieder folgendermaßen: Man findet zunächst nach (12)

$$\left(\frac{-1365}{Q}\right)=\left(\frac{5}{Q}\right)\cdot\left(\frac{3}{Q}\right)\cdot\left(\frac{7}{Q}\right)\cdot\left(\frac{13}{Q}\right)\cdot\left(\frac{-1}{Q}\right),$$

d. i. nach (20) und dem verallgemeinerten Reziprozitätsgesetze gleich

$$\left(\frac{Q}{5}\right)\cdot\left(\frac{Q}{3}\right)\cdot\left(\frac{Q}{7}\right)\cdot\left(\frac{Q}{13}\right),$$

also nach (11) gleich

$$\left(\frac{1}{5}\right)\cdot\left(\frac{1}{3}\right)\cdot\left(\frac{-1}{7}\right)\cdot\left(\frac{-2}{13}\right)=\left(\frac{-1}{7}\right)\cdot\left(\frac{-2}{13}\right)=\left(\frac{-1}{7}\right)\cdot\left(\frac{-1}{13}\right)\cdot\left(\frac{2}{13}\right),$$

d. i. nach (20) und (22) gleich $+1$.

Aus diesem Werte des Symbols $\left(\frac{-1365}{5428681}\right)$ folgt nun nicht, daß die Zahl -1365 quadratischer Rest sei von 5428681, d. h. daß die Kongruenz

$$(51) \qquad x^2 \equiv -1365 \pmod{5428681}$$

auflösbar sei. Es ist nämlich allgemein zu bemerken, daß aus $\left(\frac{P}{Q}\right) = 1$ nicht immer die Möglichkeit der Kongruenz

$$(52) \qquad x^2 \equiv P \pmod{Q}$$

hervorgeht. Dies ist zwar der Fall, so oft Q eine ungerade Primzahl ist; wenn aber

$$Q = q q' q'' \ldots$$

aus mehreren solchen zusammengesetzt ist, so kann wegen

$$(53) \qquad \left(\frac{P}{Q}\right) = \left(\frac{P}{q}\right) \cdot \left(\frac{P}{q'}\right) \cdot \left(\frac{P}{q''}\right) \ldots$$

sehr wohl $\left(\frac{P}{Q}\right) = +1$ sein, auch wenn unter den *Legendre*schen Symbolen der rechten Seite sich welche mit dem Werte -1 befinden, sobald nur deren Anzahl gerade ist; so oft aber auch nur ein einziges dieser Symbole den Wert -1 hat, muß P quadratischer Nichtrest von Q, d. h. die Kongruenz (52) unmöglich sein, denn fände sie statt, so müßte sie es auch nach jedem der Primfaktoren von Q als Modul, d. h. P müßte in bezug auf jede der Zahlen $q, q', q'' \ldots$ quadratischer Rest, die sämtlichen *Legendre*schen Symbole in (53) also $+1$ sein. — Im hier vorliegenden Falle ist aber die Kongruenz (51) wirklich lösbar und hat, wie *Gauß* (Disqu. arithm. art. 328) angegeben hat, die vier Wurzeln

$$\pm 2350978, \quad \pm 2600262.$$

Viertes Kapitel.

Die Linearform $f = ax + by$.

1. Blicken wir zurück, so werden wir leicht erkennen, daß alles, was entwickelt worden ist, wesentlich aus dem Umstande gewonnen wurde, daß, wenn a, b zwei teilerfremde Zahlen bedeuten, die Gleichung

$$(1) \qquad ax + by = 1$$

in ganzen Zahlen x, y auflösbar ist, eine Tatsache, die wir aus der Grundtatsache der Zahlentheorie (Kap. 1, Nr. 3) mittels des Modulbegriffs hergeleitet haben. Kehren wir jetzt zu jenem Ausgangspunkte noch einmal zurück.

Indem wir unter $a, b, c, \ldots$ irgend welche, nicht notwendig rationale Zahlen, unter $x, y, z, \ldots$ Unbestimmte verstehen, nennen wir den Ausdruck

$$ax + by + cz + \ldots,$$

welcher, wenn $x, y, z, \ldots$ alle ganzzahligen Werte annehmen, die Zahlen des Moduls $[a, b, c, \ldots]$ ergibt, eine Linearform, und insbesondere den Ausdruck

$$(2) \qquad f = ax + by,$$

der nur zwei Unbestimmte enthält, eine binäre Linearform. Statt der Unbestimmten x, y führen wir durch zwei Gleichungen

$$(3) \qquad x = \alpha x' + \beta y', \quad y = \gamma x' + \delta y',$$

in denen $\alpha, \beta, \gamma, \delta$ ganze Zahlen bedeuten sollen, zwei andere Unbestimmten x', y' ein; wir nennen diese Einführung oder die Gleichungen (3), durch welche sie geschieht, eine Transformation. Durch Substitution in (2) erhalten wir

$$f = a(\alpha x' + \beta y') + b(\gamma x' + \delta y') = (a\alpha + b\gamma)x' + (a\beta + b\delta)y'$$

und dürfen, wenn wir

$$(4) \qquad a\alpha + b\gamma = a', \quad a\beta + b\delta = b'$$

und

$$(5) \qquad f' = a'x' + b'y'$$

setzen, den **Satz** aussprechen:

Durch die Transformation (3) verwandelt sich die Linearform f in die Linearform f'.

Aus den Gleichungen (3) folgen aber umgekehrt diese anderen:

(6) $$\Delta x' = \delta x - \beta y\,, \qquad \Delta y' = -\gamma x + \alpha y\,,$$

in denen Δ die Determinante

(7) $$\begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix} = \alpha\delta - \beta\gamma$$

der Gleichungen (3) bedeutet, und durch sie geht f' wieder rückwärts in f über, da sich

$$a'x' + b'y' = \frac{\delta a' - \gamma b'}{\Delta} \cdot x + \frac{-\beta a' + \alpha b'}{\Delta} \cdot y$$

und aus (4)

$$\Delta a = \delta a' - \gamma b', \qquad \Delta b = -\beta a' + \alpha b'$$

ergibt.

Beschränkt man sich aber auf ganzzahlige Werte der Unbestimmten, so leuchtet ein, daß zwar ganzzahligen Werten von x', y' den Gleichungen (3) zufolge stets auch ganzzahlige Werte von x, y entsprechen, im allgemeinen aber nicht umgekehrt, da aus ganzzahligen x, y mittels der Gleichungen (6) ebensolche Werte nur für $\Delta x', \Delta y'$ gefolgert werden können. Ist $\Delta = \pm 1$, so erhalten daher mit x, y zugleich stets auch x', y' selbst ganzzahlige Werte; diese hinreichende Bedingung ist aber auch notwendig, denn, wäre Δ von ± 1 verschieden, so gingen aus (6) für $x = 1$, $y = 0$ die Werte

$$\Delta x' = \delta\,, \qquad \Delta y' = -\gamma$$

und für $x = 0$, $y = 1$ die Werte

$$\Delta x' = -\beta\,, \qquad \Delta y' = \alpha$$

hervor, und somit müßten, damit die Werte x', y' stets ganzzahlig werden, $\alpha, \beta, \gamma, \delta$ den Teiler Δ gemeinsam haben, was mit der Gleichung

$$\Delta = \alpha\delta - \beta\gamma\,,$$

deren rechte Seite dann durch Δ^2, die linke nur durch Δ teilbar wäre, sich nicht verträgt. Wir haben so den **Satz** festgestellt:

Damit vermöge der Transformation (3) ganzzahligen Werten von x', y' stets auch ganzzahlige Werte von x, y entsprechen und umgekehrt, ist notwendig und hinreichend, daß die Determinante der Transformation gleich ± 1 ist.

Da nun vermöge der Formeln (3) die Gleichheit

$$ax + by = a'x' + b'y'$$

der beiden Linearformen f, f' hergestellt wird, so wird unter der Annahme $\Delta = \pm 1$ jeder Wert, welchen die Form f für ganzzahlige x, y annimmt, einem Werte gleich sein, den die Form f' für ganzzahlige x', y' erhält und umgekehrt, oder, wie wir sagen können, die Formen f, f' stellen dann für ganzzahlige Werte ihrer Unbestimmten dieselbe Gesamtheit von Zahlen dar. Wir nennen daher zwei Linearformen f, f' einander äquivalent, wenn sie durch eine Transformation mit der Determinante ± 1 ineinander übergehen.

Nun bildet die Gesamtheit der Zahlen, welche aus der Form f mittels ganzzahliger x, y hervorgehen, den Zahlenmodul $[a, b]$ und die Gesamtheit der Zahlen, die aus f' mittels ganzzahliger x', y' entstehen, den Zahlenmodul $[a', b']$. Das gewonnene Ergebnis läßt sich daher auch so aussprechen:

Die Moduln $[a, b]$ und $[a', b']$ sind einander gleich, wenn die Beziehungen (4) statthaben, während α, β, γ, δ ganze der Bedingung

$$\alpha\delta - \beta\gamma = \pm 1 \tag{8}$$

genügende Zahlen sind. Nennt man a, b die Basis des Moduls $[a, b]$, so darf man dafür auch sagen: ein Zahlenmodul $[a, b]$ bleibt unverändert, wenn seine Basis a, b durch eine andere a', b' ersetzt wird, die mit jener durch die Gleichungen (4) und (8) verbunden ist.

2. Wir werden nun zunächst diesen Verhältnissen eine geometrische Deutung geben, die auf spätere Betrachtungen der gleichen Art vorbereiten soll.

Unter Vektor verstehen wir, wie üblich, eine Strecke AB, wenn sie nicht nur nach ihrer Größe, sondern auch nach ihrer Richtung geschätzt werden soll, so daß zwei Vektoren AB, $A'B'$ einander als gleich anzusehen sind, wenn die Strecken AB, $A'B'$ nicht nur gleiche Länge haben,

sondern auch gleich gerichtet oder doch einander gleichstimmig parallel sind. Hiernach addiert man zwei Vektoren AB, $A'B'$ (s. Fig. 1), indem man an den Endpunkt B des einen eine Strecke BC anfügt, welche mit dem andern nach Größe und Richtung identisch ist und sieht den Vektor AC als Summe beider Vektoren an.

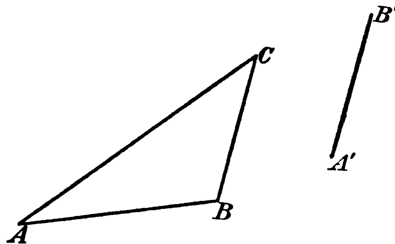


Fig. 1.

Dies vorausgeschickt, denke man nun in gewöhnlicher Weise die beiden Achsen OX, OY eines ebenen Koordinatensystems, die sich unter einem beliebig gegebenen Winkel ψ schneiden mögen, und trage nach beiden Seiten von O auf der Achse OX eine Strecke von der Größe a*), auf OY eine Strecke von der Größe b zu beliebig wiederholten Malen ab und ziehe durch die Endpunkte der aufgetragenen Strecken Parallelen je zur anderen Achse; so wird die ganze Ebene in unendlich viel kongruente Parallelogramme von der Größe $ab\sin\psi$ geteilt, und es entsteht ein sogenanntes Gitter G, dessen sämtliche Gitterpunkte, nämlich die Durchschnittspunkte beider Systeme von Parallelen, durch die Koordinaten ax, by bestimmt werden, wenn für x, y alle ganzzahligen Wertsysteme gesetzt werden. Man nennt das Gitter ein Punktgitter, wenn von den Parallelen abgesehen und nur ihre Durchschnittspunkte in Betracht gezogen werden. Faßt man aber die Strecken a, b als Vektoren und bezeichnet sie als solche durch $\bar{a}$, $\bar{b}$, so gelangt man offenbar zum Gitterpunkte mit den Koordinaten ax, by, wenn man diese seine Koordinaten als Vektoren gedacht aneinanderfügt, und daher ist deren Summe

$$\bar{a} \cdot x + \bar{b} \cdot y$$

der zum Gitterpunkte gehörige Vektor, d. i. die vom Anfangspunkte O nach ihm gezogene, nach Größe und Richtung genommene Strecke. Man ersieht aus dieser Betrachtung, daß der Gesamtheit aller Zahlen des Moduls $[a, b]$ die Gesamt-

*) Wir setzen hierbei a, b als positiv voraus.

heit der Gitterpunkte in G oder auch der ihnen zugehörigen Vektoren eindeutig entspricht: der Zahl $ax + by$ der Endpunkt des Vektors $\bar{a} \cdot x + \bar{b} \cdot y$.

Insbesondere also werden den durch die Gleichungen (4) bestimmten Zahlen a', b' dieses Moduls die Vektoren

$$(9) \qquad \overline{OA} = \bar{a} \cdot \alpha + \bar{b} \cdot \gamma, \quad \overline{OB} = \bar{a} \cdot \beta + \bar{b} \cdot \delta$$

oder ihre Endpunkte A, B mit den Koordinaten $a\alpha$, $b\gamma$; $a\beta$, $b\delta$ resp. zugeordnet sein. Nimmt man nun die Geraden, welche O mit A und mit B verbinden, zu neuen Koordinatenachsen OX', OY' und trägt auf diesen nach beiden Seiten

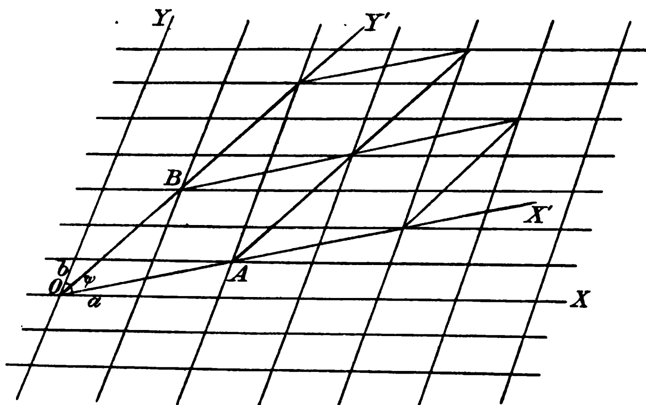


Fig. 2.

von O die Strecken OA, OB beliebig oft ab, um dann durch die Endpunkte derselben je zu der anderen Achse Parallelen zu ziehen (Fig. 2), so entsteht ein neues, aus kongruenten Parallelogrammen bestehendes Gitter G', und offenbar werden die Vektoren seiner sämtlichen Gitterpunkte erhalten, wenn in dem Ausdrucke

$$(10) \qquad \overline{OA} \cdot x' + \overline{OB} \cdot y'$$

für x', y' alle ganzen Zahlen gesetzt werden. Die Koordinaten dieser Gitterpunkte sind daher

$$a\alpha \cdot x' + a\beta \cdot y' = a(\alpha x' + \beta y') = ax,$$
$$b\gamma \cdot x' + b\delta \cdot y' = b(\gamma x' + \delta y') = by$$

und demnach jeder von ihnen ein Gitterpunkt auch von G; das gesamte Gitter G' gehört also dem Gitter G als ein Teil des letzteren an. Dies gilt nun im allgemeinen nicht auch umgekehrt; damit beide Punktgitter G und G' gänzlich aufeinanderfallen, ist — wie aus Nr. 1 einleuchtet — notwendig und hinreichend, daß die vier ganzen Zahlen $\alpha, \beta, \gamma, \delta$ die Gleichung (8) befriedigen. Denn alsdann und nur dann wird auch jeder Punkt mit den Koordinaten ax, by, d. i. jeder Gitterpunkt von G, ein Punkt mit den Koordinaten $a\alpha \cdot x' + a\beta \cdot y'$, $b\gamma \cdot x' + b\delta \cdot y'$ d. i. mit dem Vektor (10), also ein Gitterpunkt von G' sein, und somit beide Gitter sich decken. Fragt man aber nach dem geometrischen Ausdrucke dieser Bedingung, so lautet er dahin: daß die sogenannten Elementarparallelogramme beider Gitter, d. h. die aus den Seiten a, b, bzw. OA, OB gebildeten Parallelogramme gleichen Inhalt haben müssen. In der Tat ist bekanntlich der Inhalt des aus OA und OB gebildeten Parallelogrammes, ausgedrückt durch die auf OX, OY bezogenen Koordinaten der Punkte A, B gleich dem absoluten Werte von

$$(a\alpha \cdot b\delta - a\gamma \cdot b\beta) \cdot \sin\psi = (\alpha\delta - \beta\gamma) \cdot ab \sin\psi$$

und daher dem Parallelogramme $ab \sin\psi$ dann und nur dann gleich, wenn die Bedingung (8) erfüllt ist.

Aus dieser Betrachtung ersieht man, daß durch eine Transformation

$$x = \alpha x' + \beta y', \qquad y = \gamma x' + \delta y',$$

deren ganzzahlige Koeffizienten $\alpha, \beta, \gamma, \delta$ der Bedingung (8) genügen, das zur Linearform $f = ax + by$ gehörige Gitter G unverändert bleibt und nur auf eine andere Weise in Elementarparallelogramme geteilt wird.

3. Haben wir bisher die Zahlen a, b beliebig gedacht, so verstehen wir darunter nunmehr positive ganze Zahlen. In dieser Voraussetzung ist aber, wie in Kap. 1, Nr. 3, 4 gezeigt worden ist, der Modul $[a, b]$ oder, was ersichtlich dasselbe ist, der Modul $[a, -b]$ identisch mit dem eingliedrigen Modul $[d]$, in welchem d den größten gemeinsamen Teiler von a, b bedeutet, und deshalb gibt es, wenn m irgend ein Vielfaches von d, d. i. eine durch d teilbare Zahl ist, ganze Zahlen α, β, welche die Gleichung

$$a\alpha - b\beta = m \tag{11}$$

erfüllen, oder die unbestimmte Gleichung ersten Grades

$$(12) \qquad ax - by = m$$

ist in ganzen Zahlen x, y auflösbar. Daß sie auch nur dann aufgelöst werden kann, wenn m durch den größten gemeinsamen Teiler von a, b ebenfalls teilbar ist, leuchtet daraus ein, daß dieser auch in jeder Zahl von der Form $ax - by$ aufgehen muß. Hat aber die Gleichung (12) eine ganzzahlige Auflösung, so hat sie deren stets unendlich viele und sie können mit Leichtigkeit aus jener einen bestimmt werden. In der Tat, sei α, β die eine Auflösung und x, y irgend eine andere, dann bestehen die beiden Gleichungen (11) und (12) zusammen, und es ergibt sich aus ihnen die dritte:

$$ax - by = a\alpha - b\beta$$

oder $a(x - \alpha) = b(y - \beta)$, d. i., wenn $a = a'd$, $b = b'd$ gesetzt wird, wo nun a', b' teilerfremd sind,

$$a'(x - \alpha) = b'(y - \beta),$$

also $x - \alpha$ teilbar durch b', etwa $x - \alpha = b'z$ und dann $y - \beta = a'z$, wo z eine ganze Zahl bedeutet. Jede Lösung von (12) hat also die Form:

$$(13) \qquad x = \alpha + \frac{b}{d} \cdot z, \qquad y = \beta + \frac{a}{d} \cdot z.$$

Die Zahlen dieser Form stellen aber auch für jeden ganzzahligen Wert von z eine ganzzahlige Lösung der Gleichung (12) dar, da aus ihnen

$$ax - by = a\alpha - b\beta = m$$

hervorgeht. Demnach geben die Formeln (13) die vollständige Lösung der Gleichung (12) an, wenn darin für z alle ganzen Zahlen gesetzt werden. Sind insbesondere a, b teilerfremd, also $d = 1$, so ist die Gesamtheit der Vielfachen m von d mit der Gesamtheit aller ganzen Zahlen identisch; die Gleichung (12) ist dann also stets in ganzen Zahlen x, y auflösbar oder, wie man auch sagt, jede ganze Zahl m ist dann durch die Linearform $ax - by$ darstellbar, und sämtliche Darstellungen derselben oder sämtliche ganzzahligen

Auflösungen der Gleichung (12) werden aus einer derselben, α, β, durch die Formeln

(14) $$x = \alpha + bz, \quad y = \beta + az$$

gefunden, wenn in diesen z alle ganzen Zahlen durchläuft.

So hat also für teilerfremde a, b auch die Gleichung

(15) $$ax - by = 1$$

unendlich viel ganzzahlige Auflösungen, welche sämtlich in der angegebenen Weise mittels der Formeln (14) aus einer solchen Auflösung α, β zu finden sind. Man merke, daß durch passende Wahl des ganzzahligen z nach der ersten der Formeln (14) der Wert von x auf das Intervall 0 bis b beschränkt werden kann, so daß

(16a) $$0 \gtreqless x < b$$

wird; setzt man nämlich $\alpha = qb + r$, wo $0 \gtreqless r < b$ gedacht wird, so erreicht man das Gewollte, wenn $z = -q$ gewählt wird. Da nun zufolge (15)

$$1 + by = ax$$

ist, wird bei solcher Wahl von z

$$by < ab$$

also auch

(16b) $$0 \gtreqless y < a$$

sein*). Es gibt daher eine ganzzahlige Lösung der Gleichung (15), bei welcher x, y die Ungleichheiten (16a), (16b) befriedigen. Da zudem von den Werten des x nur einer zwischen 0 und b, und von den Werten des y nur einer zwischen 0 und a liegen kann, gibt es auch nur eine einzige Lösung x, y von der angegebenen Art. Fände man daher, daß eine Lösung ξ, η derselben Gleichung die Ungleichheiten

$$0 \gtreqless \xi < b, \quad 0 \gtreqless \eta < a$$

erfüllte, so müßte man daraus schließen, daß sie mit der Lösung x, y identisch sei; an späterer Stelle werden wir Veranlassung haben, auf diese Bemerkung zurückzuweisen.

---

*) Die Gleichheitszeichen in den Formeln (16a), (16b) sind nur in dem speziellen Falle $b = 1$ resp. $a = 1$ zulässig.

Endlich leuchtet ein, daß die Gleichung (12) mit der anderen:

$$\frac{a}{d}x - \frac{b}{d}y = \frac{m}{d},$$

in welcher die Koeffizienten von x, y teilerfremd sind, genau die gleichen Lösungen haben muß; deshalb darf man sich auf den Fall einer Gleichung (12) mit teilerfremden Koeffizienten beschränken. Weil alsdann aber die Gleichung (15)

$$ax - by = 1$$

auflösbar ist und aus einer ganzzahligen Auflösung α, β der letzteren sich eine solche Lösung $\alpha m, \beta m$ der Gleichung (12) und daher vermittels der Formeln

$$x = \alpha m + bz, \quad y = \beta m + az$$

sich ihre sämtlichen ganzzahligen Auflösungen ergeben, so genügt es schließlich, allein die Gleichung (15) weiter zu behandeln und ihre ganzzahligen Auflösungen zu suchen. Mithin werden wir uns fortan auf die Betrachtung dieser Gleichung beschränken.

4. Es kommt allein noch darauf an, zu zeigen, wie man eine ganzzahlige Auflösung der Gleichung (15) finden kann. Dazu könnte man zurückgreifen auf die in Kap. 2 Nr. 7 gegebene Auflösung der Kongruenzen ersten Grades. In der Tat ist die ganzzahlige Auflösung der Gleichung (15) nichts anderes als die der Kongruenz

$$(17) \qquad ax \equiv 1 \pmod{b},$$

denn, wenn x, y ganze Zahlen bedeuten, welche die Gleichung (15) erfüllen, so stellt x eine Lösung der Kongruenz (17) dar, und umgekehrt folgt aus einer solchen die Teilbarkeit von $ax - 1$ durch b, d. h. eine Zahl y, für welche $ax - by = 1$ ist. Aber, so einfach die direkte Auflösung der Kongruenz (17) für kleine Moduln b ist, so umständlich gestaltet sie sich für große, und es empfiehlt sich vielmehr, umgekehrt ihre Auflösung auf diejenige der Gleichung (15) zurückzuführen.

Weiter aber haben wir in Anknüpfung an den *Euklid*ischen Algorithmus für zwei Zahlen a, b an einem Beispiel gezeigt, wie unmittelbar aus demselben eine Auflösung der Gleichung (15) gefunden werden kann, und wir wollen diese

Methode jetzt allgemein entwickeln. Setzen wir a, b als teilerfremd, also ihren größten gemeinsamen Teiler als 1 voraus, so nimmt der *Euklid*ische Algorithmus die Form an:

$$(18)\qquad \begin{cases} a = b\alpha + b_1 \\ b = b_1\alpha_1 + b_2 \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ b_{\nu-4} = b_{\nu-3}\alpha_{\nu-3} + b_{\nu-2} \\ b_{\nu-3} = b_{\nu-2}\alpha_{\nu-2} + b_{\nu-1} \\ b_{\nu-2} = b_{\nu-1}\alpha_{\nu-1} + 1\,. \end{cases}$$

Setzt man hier in die letzte der Gleichungen, welcher die Gestalt

$$b_{\nu-2} - b_{\nu-1} \cdot \alpha_{\nu-1} = 1$$

gegeben werde, für $b_{\nu-1}$ den aus der vorletzten Gleichung entnommenen Wert, so geht sie über in

$$(19\text{a})\qquad b_{\nu-3} \cdot \alpha_{\nu-1} - b_{\nu-2}(\alpha_{\nu-2}\alpha_{\nu-1} + 1) = -1\,;$$

durch Substitution des aus der drittletzten Gleichung entnommenen Wertes für $b_{\nu-2}$ verwandelt sich diese in die folgende:

$$(19\text{b})\ b_{\nu-4}(\alpha_{\nu-2}\alpha_{\nu-1}+1) - b_{\nu-3}(\alpha_{\nu-3}(\alpha_{\nu-2}\alpha_{\nu-1}+1)+\alpha_{\nu-1}) = 1$$

usw.; allgemein ergibt sich auf solche Weise eine Formel

$$(19)\qquad b_{\nu-i} \cdot A'_{\nu-i+1} - b_{\nu-i+1} \cdot A_{\nu-i+1} = (-1)^i,$$

worin $A_{\nu-i+1}$, $A'_{\nu-i+1}$ Zahlen bedeuten, deren erste aus den Quotienten

$$\alpha_{\nu-i+1},\ \alpha_{\nu-i+2},\ \alpha_{\nu-i+3},\ \ldots,\ \alpha_{\nu-1},$$

deren zweite aus den Quotienten

$$\alpha_{\nu-i+2},\ \alpha_{\nu-i+3},\ \ldots,\ \alpha_{\nu-1}$$

durch Addition und Multiplikation gebildet und demnach, ebenso wie diese, positive ganze Zahlen sind. Um diese ihre Abhängigkeit von den Quotienten α_i anzudeuten, setzen wir

$$A_{\nu-i+1} = \{\alpha_{\nu-i+1},\ \alpha_{\nu-i+2},\ \ldots,\ \alpha_{\nu-1}\}$$
$$A'_{\nu-i+1} = \{\alpha_{\nu-i+2},\ \alpha_{\nu-i+3},\ \ldots,\ \alpha_{\nu-1}\}',$$

eine Bezeichnung, welche von *Gauß**) (Disq. arithm. art. 27) herrührt und daher *Gauß*sche Klammer genannt wird. Führt man den angedeuteten Prozeß bis zur zweiten der Gleichungen (18), d. i. bis $i = \nu$ fort, so findet sich aus (19) die Gleichung

(20) $$b \cdot A_1' - b_1 \cdot A_1 = (-1)^\nu ,$$

worin

$$A_1 = \{\alpha_1, \alpha_2, \ldots, \alpha_{\nu-1}\} ,$$

und, noch einen Schritt weitergehend bis zur ersten der Gleichungen (18), die folgende Gleichung:

(21) $$a \cdot A' - b \cdot A = (-1)^{\nu+1} ,$$

in welcher

(22) $$A = \{\alpha, \alpha_1, \alpha_2, \ldots, \alpha_{\nu-1}\}$$

zu setzen ist.

5. Es handelt sich nun darum, die fundamentalen Eigenschaften der *Gauß*schen Klammernausdrücke zu ermitteln. Zunächst ergibt sich ihr einfaches Bildungsgesetz folgendermaßen:

Stellen wir neben die Gleichungen (18) die folgenden:

(23) $$\begin{cases} x = \alpha y + y_1 \\ y = \alpha_1 y_1 + y_2 \\ \cdots\cdots\cdots\cdots \\ y_{\nu-3} = \alpha_{\nu-2} y_{\nu-2} + y_{\nu-1} \\ y_{\nu-2} = \alpha_{\nu-1} y_{\nu-1} + y_\nu , \end{cases}$$

so werden, wenn x, y nach Belieben gewählt werden, auch alle folgenden Größen $y_1, y_2, \ldots, y_\nu$ durch jene Gleichungen mitbestimmt sein. Aus diesen letzteren ergibt sich aber auf gleiche Weise, wie die Formel (21) aus den Gleichungen (18), die Beziehung

(24) $$x \cdot A' - y \cdot A = (-1)^{\nu+1} \cdot y_\nu$$

und, wenn man den gleichen Prozeß, doch erst von der vorletzten der Gleichungen (23) aus wiederholt, diese analoge:

(24a) $$x \cdot B' - y \cdot B = (-1)^\nu \cdot y_{\nu-1} ,$$

*) *Gauß* benutzt eckige Klammern; um Verwechslung mit dem Modulzeichen zu vermeiden, ist hier das andere Klammernzeichen gewählt.

endlich, wenn man erst mit der drittletzten Gleichung beginnt, die Beziehung

$$(24\text{b}) \qquad x \cdot \Gamma' - y \cdot \Gamma = (-1)^{\nu-1} \cdot y_{\nu-2},$$

wo nun

$$B = \{\alpha, \alpha_1, \alpha_2, \ldots, \alpha_{\nu-2}\}$$
$$\Gamma = \{\alpha, \alpha_1, \alpha_2, \ldots, \alpha_{\nu-3}\}$$

sind. Diese drei Beziehungen mit Rücksicht auf die letzte der Gleichungen (23) verbindend, gewinnt man die folgende:

$$x \cdot \Gamma' - y \cdot \Gamma = x \cdot (A' - \alpha_{\nu-1} \cdot B') - y \cdot (A - \alpha_{\nu-1} \cdot B),$$

derzufolge, da die Unbestimmten x, y beliebig gewählt werden können, etwa einmal gleich 1, 0, ein zweites Mal gleich 0, 1,

$$\Gamma = A - \alpha_{\nu-1} \cdot B, \qquad \Gamma' = A' - \alpha_{\nu-1} \cdot B',$$

also

$$A = \alpha_{\nu-1} \cdot B + \Gamma,$$

d. i. mit Beachtung der Ausdrücke für A, B, Γ nachstehendes Bildungsgesetz:

$$(25) \quad \begin{cases} \{\alpha, \alpha_1, \alpha_2, \ldots, \alpha_{\nu-1}\} = \{\alpha, \alpha_1, \alpha_2, \ldots, \alpha_{\nu-2}\} \cdot \alpha_{\nu-1} \\ \qquad\qquad + \{\alpha, \alpha_1, \alpha_2, \ldots, \alpha_{\nu-3}\} \end{cases}$$

gefunden wird.

Andererseits erhält man aus den Gleichungen (23) neben der Formel (24), welche (21) entspricht, der Gleichung (20) entsprechend die folgende:

$$y \cdot A_1' - y_1 \cdot A_1 = (-1)^{\nu} \cdot y_{\nu},$$

d. i. wegen $y_1 = x - \alpha y$ die Gleichung

$$x \cdot A_1 - (A_1' + \alpha A_1) \cdot y = (-1)^{\nu+1} \cdot y_{\nu},$$

deren Vergleichung mit (24) die weiteren Beziehungen

$$A_1 = A', \qquad A = A_1' + \alpha A_1$$

ergibt. Die erstere derselben lehrt, daß auch der Koeffizient A' eine *Gauß*sche Klammerngröße wie A ist, nämlich

$$A' = \{\alpha_1, \alpha_2, \ldots, \alpha_{\nu-1}\}$$

und demnach, da A_1' zu A_1 in derselben Beziehung steht wie A' zu A, auch

$$A_1' = \{\alpha_2, \alpha_3, \ldots, \alpha_{\nu-1}\}$$

ist; während nun die zweite ein neues, der Formel (25) ähnliches Bildungsgesetz für diese Klammerngrößen liefert, nach welchem

$$(26)\quad \begin{cases} \{\alpha, \alpha_1, \alpha_2, \ldots, \alpha_{\nu-1}\} = \alpha \cdot \{\alpha_1, \alpha_2, \ldots, \alpha_{\nu-1}\} \\ \qquad\qquad + \{\alpha_2, \alpha_3, \ldots, \alpha_{\nu-1}\} \end{cases}$$

ist.

6. Die Verbindung der Formeln (25) und (26) miteinander gestattet sogleich eine dritte Eigenschaft der *Gauß*schen Klammern zu erhärten, welche in der Gleichheit

$$(27)\quad \{\alpha, \alpha_1, \alpha_2, \ldots, \alpha_{\nu-1}\} = \{\alpha_{\nu-1}, \alpha_{\nu-2}, \ldots, \alpha_1, \alpha\}$$

ihren Ausdruck findet, man darf also die Reihe der Quotienten umkehren. Nach (19a) ist

$$\{\alpha_{\nu-2}, \alpha_{\nu-1}\} = \alpha_{\nu-2}\alpha_{\nu-1} + 1,$$

ebenso würde

$$\{\alpha_{\nu-1}, \alpha_{\nu-2}\} = \alpha_{\nu-1}\alpha_{\nu-2} + 1$$

sein und daher steht die Gleichung (27) für zwei Elemente bereits fest:

$$\{\alpha_{\nu-2}, \alpha_{\nu-1}\} = \{\alpha_{\nu-1}, \alpha_{\nu-2}\}.$$

Nehmen wir an, sie sei schon allgemeiner für weniger als ν Elemente festgestellt, so darf man die Gleichung (26) auch folgendermaßen schreiben:

$$\{\alpha, \alpha_1, \alpha_2, \ldots, \alpha_{\nu-1}\} = \{\alpha_{\nu-1}, \alpha_{\nu-2}, \ldots, \alpha_2, \alpha_1\} \cdot \alpha + \{\alpha_{\nu-1}, \alpha_{\nu-2}, \ldots, \alpha_3, \alpha_2\},$$

wo nun die rechte Seite auf Grund des Gesetzes (25) durch

$$\{\alpha_{\nu-1}, \alpha_{\nu-2}, \ldots, \alpha_2, \alpha_1, \alpha\}$$

ersetzt werden darf; demnach gilt dann die Formel (27) auch für ν Elemente und somit allgemein.

Eine fernere Eigenschaft lehrt die Formel

$$(28)\quad \begin{cases} \{-\alpha, -\alpha_1, -\alpha_2, \ldots, -\alpha_{\nu-1}\} \\ = (-1)^\nu \cdot \{\alpha, \alpha_1, \alpha_2, \ldots, \alpha_{\nu-1}\}, \end{cases}$$

die ebenfalls durch allgemeine Induktion bewiesen wird. In der Tat ist

$$\{-\alpha_{\nu-2}, -\alpha_{\nu-1}\} = \alpha_{\nu-2}\alpha_{\nu-1} + 1 = \{\alpha_{\nu-2}, \alpha_{\nu-1}\},$$

die Formel (28) besteht also für zwei Elemente; wird nun vorausgesetzt, daß sie bereits allgemeiner für weniger als ν Elemente bewiesen sei, so liefert die Formel (26) zunächst

$$\{-\alpha, -\alpha_1, -\alpha_2, \ldots, -\alpha_{\nu-1}\} = -\alpha \cdot \{-\alpha_1, -\alpha_2, \ldots, -\alpha_{\nu-1}\} + \{-\alpha_2, \ldots, -\alpha_{\nu-1}\},$$

also nach der Voraussetzung gleich

$$(-1)^{\nu} \cdot \alpha \{\alpha_1, \alpha_2, \ldots, \alpha_{\nu-1}\} + (-1)^{\nu-2} \cdot \{\alpha_2, \ldots, \alpha_{\nu-1}\},$$

d. h. wieder nach (26) gleich

$$(-1)^{\nu} \cdot \{\alpha, \alpha_1, \alpha_2, \ldots, \alpha_{\nu-1}\},$$

die Formel (28) besteht dann also auch für ν Elemente und ist auf solche Weise als allgemein bewiesen.

Endlich schreiben wir die Gleichungen (23) in umgekehrter Reihenfolge auf nachstehende Weise:

$$\begin{aligned}
y_\nu &= -\alpha_{\nu-1} y_{\nu-1} + y_{\nu-2} \\
y_{\nu-1} &= -\alpha_{\nu-2} y_{\nu-2} + y_{\nu-3} \\
&\ldots\ldots\ldots\ldots \\
y_2 &= -\alpha_1 y_1 + y \\
y_1 &= -\alpha y + x.
\end{aligned}$$

Entsprechend der aus den ursprünglichen Gleichungen (23) gefolgerten Beziehung (24) und bei Berücksichtigung des Klammernausdruckes für A' geht hieraus die Beziehung

$$y_\nu \cdot \{-\alpha_{\nu-2}, -\alpha_{\nu-3}, \ldots, -\alpha_1, -\alpha\} - y_{\nu-1} \cdot \{-\alpha_{\nu-1}, -\alpha_{\nu-2}, \ldots, -\alpha_1, -\alpha\} = (-1)^{\nu+1} \cdot x$$

oder

$$\text{(29a)} \quad \begin{cases} y_\nu \cdot \{\alpha_{\nu-2}, \alpha_{\nu-3}, \ldots, \alpha_1, \alpha\} \\ + y_{\nu-1} \cdot \{\alpha_{\nu-1}, \alpha_{\nu-2}, \ldots, \alpha_1, \alpha\} = x \end{cases}$$

hervor, während aus den Formeln (24), (24a) durch die Elimination von y die andere:

$$\text{(29b)} \quad y_\nu \cdot B + y_{\nu-1} \cdot A = (-1)^{\nu+1} \cdot (A'B - B'A) \cdot x$$

gefunden wird. Hierin ist

$$\begin{aligned}
A &= \{\alpha, \alpha_1, \ldots, \alpha_{\nu-1}\} = \{\alpha_{\nu-1}, \alpha_{\nu-2}, \ldots, \alpha_1, \alpha\} \\
A' &= \{\alpha_1, \alpha_2, \ldots, \alpha_{\nu-1}\} \\
B &= \{\alpha, \alpha_1, \ldots, \alpha_{\nu-2}\} = \{\alpha_{\nu-2}, \ldots, \alpha_1, \alpha\},
\end{aligned}$$

also

$$B' = \{\alpha_1, \alpha_2, \ldots, \alpha_{\nu-2}\}.$$

Da somit die Koeffizienten von $y_{\nu-1}$, y_ν in den beiden Formeln (29a), (29b) übereinstimmen, erschließt man auch die Gleichheit der Koeffizienten von x und folglich die wichtige Beziehung

$$(30)\quad \left\{\begin{aligned} &\{\alpha, \alpha_1, \alpha_2, \ldots, \alpha_{\nu-1}\}\cdot\{\alpha_1, \alpha_2, \ldots, \alpha_{\nu-2}\}\\ &-\{\alpha, \alpha_1, \alpha_2, \ldots, \alpha_{\nu-2}\}\cdot\{\alpha_1, \alpha_2, \ldots, \alpha_{\nu-1}\}\\ &\qquad\qquad = (-1)^\nu. \end{aligned}\right.$$

7. Die *Gauß*schen Klammern haben eine besondere Bedeutung für die gewöhnliche Kettenbruchentwicklung des rationalen Bruchs $\frac{a}{b}$, wie denn der *Euklid*ische Algorithmus für a, b unmittelbar zu dieser Kettenbruchentwicklung führt. Denn aus den Gleichungen (18) desselben schließt man die folgenden:

$$\begin{aligned} \frac{a}{b} &= \alpha + \frac{b_1}{b}\\ \frac{b}{b_1} &= \alpha_1 + \frac{b_2}{b_1}\\ \frac{b_1}{b_2} &= \alpha_2 + \frac{b_3}{b_2}\\ &\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\\ \frac{b_{\nu-3}}{b_{\nu-2}} &= \alpha_{\nu-2} + \frac{b_{\nu-1}}{b_{\nu-2}}\\ \frac{b_{\nu-2}}{b_{\nu-1}} &= \alpha_{\nu-1} + \frac{1}{b_{\nu-1}} \end{aligned}$$

und nunmehr durch allmähliche Substitutionen in die erste dieser Formeln den Kettenbruch

$$(31)\quad \frac{a}{b} = \alpha + \cfrac{1}{\alpha_1 + \cfrac{1}{\alpha_2 + \cdots + \cfrac{1}{\alpha_{\nu-2} + \cfrac{1}{\alpha_{\nu-1} + \cfrac{1}{\alpha_\nu}}}}},$$

wo α_ν für $b_{\nu-1}$ gesetzt, der letzten der Gleichungen (18) nämlich noch eine weitere Gleichung

$$b_{\nu-1} = 1\cdot\alpha_\nu$$

hinzugefügt ist. Um die unbequeme Schreibweise solcher Brüche zu vermeiden und Raum zu sparen, wollen wir fortan für diesen Kettenbruch das Zeichen

$$\frac{a}{b} = \lfloor \alpha, \alpha_1, \alpha_2, \ldots, \alpha_{\nu-1}, \alpha_\nu \rceil \tag{32}$$

verwenden. Bricht man ihn bei seinen einzelnen Teilnennern $\alpha_1, \alpha_2, \ldots, \alpha_{\nu-1}, \alpha_\nu$ ab, so erhält man seine aufeinanderfolgenden sogenannten Näherungsbrüche

$$\alpha = \lfloor \alpha \rceil, \qquad \alpha + \frac{1}{\alpha_1} = \lfloor \alpha, \alpha_1 \rceil,$$

$$\alpha + \cfrac{1}{\alpha_1 + \cfrac{1}{\alpha_2}} = \lfloor \alpha, \alpha_1, \alpha_2 \rceil$$

usw. Jeder von diesen läßt sich wieder in die Form eines gewöhnlichen rationalen Bruches zurückführen:

$$(33) \quad \begin{cases} \alpha = \dfrac{\alpha}{1}, \qquad \alpha + \dfrac{1}{\alpha_1} = \dfrac{\alpha\alpha_1 + 1}{\alpha_1}, \\[2ex] \alpha + \cfrac{1}{\alpha_1 + \cfrac{1}{\alpha_2}} = \dfrac{\alpha(\alpha_1\alpha_2 + 1) + \alpha_2}{\alpha_1\alpha_2 + 1} \end{cases}$$

usw. Schon hier sieht man Ausdrücke erscheinen, die durch Vergleichung mit den Koeffizienten der Formeln (19a), (19b) als *Gauß*sche Klammern erkannt werden. In der Tat zeigt man leicht, daß der Kettenbruch

$$\lfloor \alpha, \alpha_1, \alpha_2, \ldots, \alpha_{i-1} \rceil$$

gleich dem Quotienten zweier *Gauß*scher Klammern:

$$\lfloor \alpha, \alpha_1, \alpha_2, \ldots, \alpha_{i-1} \rceil = \frac{\{\alpha, \alpha_1, \alpha_2, \ldots, \alpha_{i-1}\}}{\{\alpha_1, \alpha_2, \ldots, \alpha_{i-1}\}} \tag{34}$$

ist. Dies stimmt den Gleichungen (33) zufolge für Kettenbrüche mit zwei und mit drei Gliedern; wir wollen annehmen, es sei allgemeiner bereits für solche mit weniger als i Gliedern bewiesen. Da nun

$$\lfloor \alpha, \alpha_1, \alpha_2, \ldots, \alpha_{i-1} \rceil = \alpha + \frac{1}{\lfloor \alpha_1, \alpha_2, \ldots, \alpha_{i-1} \rceil}$$

und nach der gemachten Annahme

$$\lfloor \alpha_1, \alpha_2, \ldots, \alpha_{i-1} \rceil = \frac{\{\alpha_1, \alpha_2, \ldots, \alpha_{i-1}\}}{\{\alpha_2, \ldots, \alpha_{i-1}\}}$$

ist, so ergibt sich

$$\lfloor \alpha, \alpha_1, \alpha_2, \ldots, \alpha_{i-1} \rceil = \alpha + \frac{\{\alpha_2, \alpha_3, \ldots, \alpha_{i-1}\}}{\{\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_{i-1}\}}$$

$$= \frac{\alpha \cdot \{\alpha_1, \alpha_2, \ldots, \alpha_{i-1}\} + \{\alpha_2, \alpha_3, \ldots, \alpha_{i-1}\}}{\{\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_{i-1}\}},$$

d. h. nach dem allgemeinen Bildungsgesetze (26) für die *Gauß*schen Klammern gleich

$$\frac{\{\alpha, \alpha_1, \alpha_2, \ldots, \alpha_{i-1}\}}{\{\alpha_1, \alpha_2, \ldots, \alpha_{i-1}\}},$$

und somit erhält man die Formel (34), deren allgemeine Gültigkeit auf solche Weise erwiesen ist.

8. Dieser Nachweis und das Bildungsgesetz (25) der *Gauß*schen Klammern gibt nun einen einfachen Algorithmus an die Hand, die sukzessiven Näherungsbrüche des Kettenbruchs (31) zu bilden. Man setze allgemein den $i$ten Näherungsbruch

$$(35) \qquad \lfloor \alpha, \alpha_1, \alpha_2, \ldots, \alpha_{i-1} \rceil = \frac{z_i}{n_i},$$

indem man unter z_i, n_i ganze Zahlen ohne gemeinsamen Teiler versteht. Dann schreibe man die Reihe der Teilnenner des Kettenbruchs (31)

$$(36) \qquad 1, \alpha, \alpha_1, \alpha_2, \ldots, \alpha_{i-1}, \ldots, \alpha_{\nu-1}, \alpha_\nu,$$

denen man die Glieder 1 und das Anfangsglied α voranstelle, und unter sie die Brüche

$$\frac{z_0}{n_0}, \frac{z_1}{n_1}, \frac{z_2}{n_2}, \ldots \frac{z_i}{n_i}, \ldots \frac{z_\nu}{n_\nu}, \frac{z_{\nu+1}}{n_{\nu+1}},$$

als deren beide ersten

$$\frac{z_0}{n_0} = \frac{1}{0}, \quad \frac{z_1}{n_1} = \frac{\alpha}{1}$$

gewählt werden (der Bruch $\frac{1}{0}$ ist dabei rein in formalem Sinne zu nehmen, da ihm kein Wert zukommt). Alsdann findet

man einfach Zähler und Nenner des $i$ten Näherungsbruches $\frac{z_i}{n_i}$ vom zweiten an gerechnet, indem man den Zähler resp. Nenner des $i-1$ten Näherungsbruches mit dem Teilnenner α_{i-1} multipliziert und dazu den Zähler resp. Nenner des $i-2$ten Näherungsbruches hinzufügt. Denn die Vergleichung der Formeln (34) und (35) ergibt, da die *Gauß*schen Klammern in der ersteren von ihnen wegen (30) teilerfremd sind, ebenso wie z_i, n_i, die Gleichheiten

(37) $$\begin{cases} z_i = \{\alpha, \alpha_1, \alpha_2, \ldots, \alpha_{i-1}\} \\ n_i = \{\alpha_1, \alpha_2, \ldots, \alpha_{i-1}\}, \end{cases}$$

also nach (25)

$$z_i = \{\alpha, \alpha_1, \ldots, \alpha_{i-2}\} \cdot \alpha_{i-1} + \{\alpha, \alpha_1, \ldots, \alpha_{i-3}\}$$
$$n_i = \{\alpha_1, \alpha_2, \ldots, \alpha_{i-2}\} \cdot \alpha_{i-1} + \{\alpha_1, \alpha_2, \ldots, \alpha_{i-3}\}$$

oder

(38) $$\begin{cases} z_i = \alpha_{i-1} \cdot z_{i-1} + z_{i-2} \\ n_i = \alpha_{i-1} \cdot n_{i-1} + n_{i-2}. \end{cases}$$

Nimmt man z. B.

$$a = 1126, \quad b = 253,$$

also

$$1126 = 3 \cdot 353 + 67$$
$$353 = 5 \cdot 67 + 18$$
$$67 = 3 \cdot 18 + 13$$
$$18 = 1 \cdot 13 + 5$$
$$13 = 2 \cdot 5 + 3$$
$$5 = 1 \cdot 3 + 2$$
$$3 = 1 \cdot 2 + 1$$
$$2 = 2 \cdot 1$$

und

(39) $$\frac{1126}{353} = \lfloor 3, 5, 3, 1, 2, 1, 1, 2 \rceil,$$

so erhält man das Schema:

$$\begin{matrix} 1, & 3, & 5, & 3, & 1, & 2, & 1, & 1, & 2 \\ \frac{1}{0}, & \frac{3}{1}, & \frac{z_2}{n_2}, & \frac{z_3}{n_3}, & \frac{z_4}{n_4}, & \frac{z_5}{n_5}, & \frac{z_6}{n_6}, & \frac{z_7}{n_7}, & \frac{z_8}{n_8} \end{matrix}$$

und aus obiger Regel

$$z_2 = 5 \cdot 3 + 1 = 16 \qquad n_2 = 5 \cdot 1 + 0 = 5$$
$$z_3 = 3 \cdot 16 + 3 = 51 \qquad n_3 = 3 \cdot 5 + 1 = 16$$
$$z_4 = 1 \cdot 51 + 16 = 67 \qquad n_4 = 1 \cdot 16 + 5 = 21$$
$$z_5 = 2 \cdot 67 + 51 = 185 \qquad n_5 = 2 \cdot 21 + 16 = 58$$
$$z_6 = 1 \cdot 185 + 67 = 252 \qquad n_6 = 1 \cdot 58 + 21 = 79$$
$$z_7 = 1 \cdot 252 + 185 = 437 \qquad n_7 = 1 \cdot 79 + 58 = 137$$
$$z_8 = 2 \cdot 437 + 252 = 1126 \qquad n_8 = 2 \cdot 137 + 79 = 353.$$

Die Reihe der Näherungsbrüche für den Kettenbruch (39) ist daher die folgende:

$$\frac{3}{1}, \frac{16}{5}, \frac{51}{16}, \frac{67}{21}, \frac{185}{58}, \frac{252}{79}, \frac{437}{137}, \frac{1126}{353},$$

deren letzter, wie es sein muß, mit dem Werte des ganzen Kettenbruches übereinkommt.

9. Die bisher betrachteten Kettenbrüche bestanden stets aus einer endlichen Anzahl von Gliedern. Bedeutet aber

$$\alpha, \alpha_1, \alpha_2, \alpha_3, \alpha_4, \ldots$$

eine Reihe von positiven ganzen Zahlen, die nach irgend einer vorgeschriebenen Regel unbegrenzt fortgesetzt werden kann, so läßt sich dementsprechend auch ein Kettenbruch

(40) $$\Omega = \lfloor \alpha, \alpha_1, \alpha_2, \alpha_3, \alpha_4, \ldots \rceil$$

aufstellen, der aus einer unbegrenzten Menge von Gliedern besteht. Da ein solcher, an einer beliebigen Stelle abgebrochen, wieder zu einem endlichen wird, so werden die Gesetze, die soeben für die Näherungsbrüche im letzteren Falle abgeleitet worden sind, auch für die Näherungsbrüche des unendlichen Kettenbruchs gelten. Aber es fragt sich, ob diesem ein bestimmter Sinn zukommt, demgemäß er als eine Zahlengröße angesehen werden darf.

In dieser Hinsicht bemerke man, daß auf Grund der für *Gauß*sche Klammern erwiesenen Gleichung (30) zwischen den Zählern und Nennern zweier aufeinanderfolgenden Näherungsbrüche $\frac{z_{i-1}}{n_{i-1}}, \frac{z_i}{n_i}$ die Beziehung

(41) $$z_i \cdot n_{i-1} - n_i \cdot z_{i-1} = (-1)^i$$

besteht, aus welcher die andere:

$$(42) \qquad \frac{z_i}{n_i} - \frac{z_{i-1}}{n_{i-1}} = \frac{(-1)^i}{n_{i-1}\, n_i}$$

hervorgeht. Da nun die Größen z_i, n_i als Werte von *Gauß*schen Klammern positive ganze Zahlen sind, so hat die rechte Seite dieser Gleichung einen positiven oder negativen Wert, je nachdem i gerade oder ungerade ist. Man schließt also, daß jeder Näherungsbruch gerader Ordnung größer ist als der ihm voraufgehende Näherungsbruch ungerader Ordnung. Verbindet man ferner die Gleichung (42) mit der durch Verwandlung von i in $i+1$ daraus hervorgehenden Gleichung

$$\frac{z_{i+1}}{n_{i+1}} - \frac{z_i}{n_i} = \frac{(-1)^{i+1}}{n_i\, n_{i+1}}$$

durch Addition, so findet man

$$(43) \qquad \frac{z_{i+1}}{n_{i+1}} - \frac{z_{i-1}}{n_{i-1}} = \frac{(-1)^i}{n_i}\left(\frac{1}{n_{i-1}} - \frac{1}{n_{i+1}}\right),$$

wo die Klammer zur Rechten einen positiven Wert hat, da Zähler und Nenner der Näherungsbrüche der Bildung der *Gauß*schen Klammern oder den Formeln (38) zufolge offenbar mit zunehmendem Index i fortwährend und zwar über jede Grenze hinaus wachsen. Ist also i ungerade, so ist der Unterschied (43) der beiden Näherungsbrüche negativ, d. h. die Näherungsbrüche gerader Ordnung

$$(44) \qquad \frac{z_2}{n_2}, \quad \frac{z_4}{n_4}, \quad \frac{z_6}{n_6}, \quad \frac{z_8}{n_8}, \ldots$$

bilden eine unbegrenzte Reihe a b n e h m e n d e r rationaler Werte; für gerades i aber wird der Unterschied (43) positiv sein, d. h. die Näherungsbrüche ungerader Ordnung

$$(45) \qquad \frac{z_1}{n_1}, \quad \frac{z_3}{n_3}, \quad \frac{z_5}{n_5}, \quad \frac{z_7}{n_7}, \ldots$$

bilden eine unbegrenzte Reihe w a c h s e n d e r rationaler Werte. Da zudem, wie gezeigt, die Glieder der letzteren Reihe stets kleiner sind, als die entsprechenden Glieder der ersteren Reihe und ihr Unterschied gegen diese der Formel (42) zufolge mit wachsendem i unendlich abnimmt, so sind die beiden Reihen (44) und (45) zusammengenommen z w e i gegen-

einander konvergierende Wertreihen*), die miteinander einen endlichen Grenzwert definieren. Dieser Grenzwert ist als der Wert des unendlichen Kettenbruchs Ω zu betrachten.

10. Im Vorstehenden liegt zugleich der Grund für die Bezeichnung der Brüche $\frac{z_i}{n_i}$ als Näherungsbrüche des Kettenbruchs. In dem besonderen Falle, wo dieser nur ein endlicher ist, nähern sich jene Brüche, diejenigen gerader Ordnung stets wachsend, diejenigen ungerader Ordnung stets abnehmend, dem Werte $\frac{a}{b}$ des Kettenbruchs, bis der letzte von ihnen mit diesem Werte selber zusammenfällt.

Man hat demnach für den Kettenbruch (31) die Gleichung

$$\frac{z_{\nu+1}}{n_{\nu+1}} = \frac{a}{b},$$

und da Zähler und Nenner sowohl des einen wie des andern dieser Brüche teilerfremde positive Zahlen sind, jene nach der Definition, diese nach der Voraussetzung, müssen die Gleichungen bestehen:

$$z_{\nu+1} = a, \quad n_{\nu+1} = b.$$

Da aber nach der allgemeinen Formel (41)

$$z_{\nu+1} \cdot n_\nu - z_\nu \cdot n_{\nu+1} = (-1)^{\nu+1}$$

ist, läßt sich auch schreiben

$$a \cdot n_\nu - b \cdot z_\nu = (-1)^{\nu+1}$$

und hieraus findet sich sogleich eine Auflösung der Gleichung

$$(46) \qquad ax - by = 1$$

in ganzen Zahlen, indem man

$$(47) \qquad x = (-1)^{\nu+1} \cdot n_\nu, \quad y = (-1)^{\nu+1} \cdot z_\nu$$

setzt. Man erhält also folgende einfache Regel, um eine Auflösung der Gleichung (46) zu ermitteln:

Man entwickle den Bruch $\frac{a}{b}$ in einen gewöhnlichen Kettenbruch und bilde für diesen seinen vorletzten Näherungs-

*) Vgl. des Verf. Vorlesungen über die Natur der Irrationalzahlen, Leipzig, 1892, S. 7 ff.

bruch; ist dieser $\frac{z_\nu}{n_\nu}$, so geben die Formeln (47) die gesuchte Lösung.

Hierbei kann man sich immer so einrichten, daß eine Lösung in positiven Zahlen erreicht wird. Dies geschieht gewiß, wenn ν ungerade ist; wäre aber ν gerade und daher die durch (47) gegebene Auflösung eine solche in negativen Zahlen, so läßt sich der Kettenbruch (31) so abändern, daß die Anzahl seiner Teilnenner um eine Einheit kleiner oder größer wird, ν also durch $\nu - 1$ oder $\nu + 1$ ersetzt wird; wenn dann die angegebene Regel auf diesen abgeänderten Kettenbruch angewendet wird, so ergibt sich eine Auflösung in positiven Zahlen. In der Tat kann man im Kettenbruche (31) statt der zwei Glieder

$$\alpha_{\nu-1} + \frac{1}{\alpha_\nu},$$

falls $\alpha_\nu = 1$ ist, ein einzelnes Glied $(\alpha_{\nu-1} + 1)$, ist aber $\alpha_\nu > 1$, die drei Glieder

$$\alpha_{\nu-1} + \cfrac{1}{(\alpha_\nu - 1) + \cfrac{1}{1}}$$

schreiben.

Liegt z. B. die Gleichung

$$1126\,x - 353\,y = 1$$

zu lösen vor, so bilde man den Kettenbruch (39), als dessen vorletzter Näherungsbruch

$$\frac{z_7}{n_7} = \frac{437}{137}$$

gefunden worden ist; daraus ergibt sich die Lösung

$$x = 137\,, \qquad y = 437$$

in positiven ganzen Zahlen. Schriebe man dagegen den Kettenbruch (39) in der Gestalt

$$\lfloor 3,\ 5,\ 3,\ 1,\ 2,\ 1,\ 1,\ 1,\ 1 \rceil,$$

so träten an Stelle der beiden letzten Näherungsbrüche $\frac{437}{137}$, $\frac{1126}{353}$ jetzt diese drei:

$$\frac{437}{137},\quad \frac{689}{216},\quad \frac{1126}{353}$$

und man erhielte eine Auflösung

$$x = -216\,, \qquad y = -689$$

in negativen Zahlen.

11. Wir kehren nunmehr zu den linearen Transformationen von der Form

$$x = \alpha x' + \beta y', \qquad y = \gamma x' + \delta y' \tag{48}$$

wieder zurück. Für unsere späteren Betrachtungen sind diejenigen von ihnen von besonderer Wichtigkeit, welche man **unimodular** nennt, bei welchen nämlich die ganzzahligen Koeffizienten $\alpha, \beta, \gamma, \delta$ die Bedingung

$$\alpha\delta - \beta\gamma = \pm 1 \tag{49}$$

erfüllen. Man sieht, daß bei diesen α, γ teilerfremd sein müssen; hat man aber für α, γ irgend ein Paar solcher Zahlen gewählt, so hat die Gleichung

$$\alpha x - \gamma y = 1$$

unendlich viel ganzzahlige Auflösungen, die wir sämtlich den vorstehenden Betrachtungen gemäß finden können, und jede von ihnen: $x = \delta$, $y = \beta$, liefert, mit passendem Vorzeichen genommen, eine der unimodularen Transformationen, deren Anzahl also ebenfalls unendlich groß ist.

Setzt man das Verhältnis $\frac{x}{y}$ der beiden Unbestimmten x, y gleich ω, und ebenso $\frac{x'}{y'} = \omega'$, so ergibt sich zwischen diesen Größen ω, ω' den Gleichungen (48) zufolge die Beziehung

$$\omega = \frac{\alpha\omega' + \beta}{\gamma\omega' + \delta}, \tag{50}$$

mittels deren statt der Größe ω die Größe ω' eingeführt oder diese an der ersteren Stelle gesetzt wird, und die wir daher **eine lineare Substitution** nennen wollen. Setzt man nun ebenso

$$\omega' = \frac{\alpha'\omega'' + \beta'}{\gamma'\omega'' + \delta'} \tag{51}$$

und trägt diesen Wert in die Formel (50) ein, so findet man leicht die Gleichung

$$\omega = \frac{\alpha''\omega'' + \beta''}{\gamma''\omega'' + \delta''}, \tag{52}$$

worin

(53) $$\begin{cases} \alpha'' = \alpha\alpha' + \beta\gamma', & \beta'' = \alpha\beta' + \beta\delta' \\ \gamma'' = \gamma\alpha' + \delta\gamma', & \delta'' = \gamma\beta' + \delta\delta' \end{cases}$$

ist; auch ergibt sich aus diesen Werten von α'', β'', γ'', δ'' ohne Mühe die Beziehung

(54) $$\alpha''\delta'' - \beta''\gamma'' = (\alpha\delta - \beta\gamma)\cdot(\alpha'\delta' - \beta'\gamma').$$

Man erkennt solcherweise, daß durch Zusammensetzung zweier linearen Substitutionen (50), (51), d. h., wenn man auf die erstere die andere folgen läßt, wieder eine ebensolche Substitution (52) entsteht, was wir kurz ausdrücken, indem wir sagen: das Produkt zweier Linearsubstitutionen ist stets wieder eine solche. Man sagt auch statt dessen, die Gesamtheit aller Linearsubstitutionen bilde eine Gruppe. Dasselbe gilt aber auch, wenn wir aus der gesamten Menge aller Linearsubstitutionen nur diejenigen ausscheiden, bei welchen die ganzzahligen Koeffizienten α, β, γ, δ die Bedingung (49) erfüllen, nämlich für die Gesamtheit aller unimodularen Linearsubstitutionen: auch diese für sich bilden eine Gruppe. In der Tat, sind (50), (51) irgend zwei von ihnen, also

$$\alpha\delta - \beta\gamma = \pm 1, \quad \alpha'\delta' - \beta'\gamma' = \pm 1,$$

so ist auch ihr Produkt (52) eine von ihnen, da dann wegen (54) auch α'', β'', γ'', δ'' ganze Zahlen sind, welche die Bedingung

$$\alpha''\delta'' - \beta''\gamma'' = \pm 1$$

erfüllen.

12. Alle diejenigen Substitutionen dieser engeren Gruppe, bei denen α, β, γ, δ positive, der Bedingung $\alpha\delta - \beta\gamma = 1$ genügende ganze Zahlen sind, lassen sich aus zwei fundamentalen oder erzeugenden Substitutionen zusammensetzen. Um dies zu zeigen, unterscheiden wir diese unimodularen Substitutionen (50) in zwei Kategorien, je nachdem in ihnen $\alpha > \beta$ oder $\alpha < \beta$ ist. Entwickeln wir im ersteren Falle den Bruch $\frac{\alpha}{\gamma}$ in einen gewöhnlichen Kettenbruch, welcher

(55) $$\frac{\alpha}{\gamma} = \lfloor \lambda, \lambda_1, \lambda_2, \ldots, \lambda_{\nu-1} \rceil$$

sein möge, so daß $\frac{z_\nu}{n_\nu} = \frac{\alpha}{\gamma}$ und genauer $z_\nu = \alpha$, $n_\nu = \gamma$ sei; dabei dürfen wir einer Bemerkung in Nr. 10 zufolge ν als eine gerade Zahl voraussetzen. Nach der Bildungsweise der Näherungsbrüche ergibt sich dann

$$(56)\quad \lfloor \lambda, \lambda_1, \lambda_2, \ldots, \lambda_{\nu-1}, \omega' \rceil = \frac{z_\nu \omega' + z_{\nu-1}}{n_\nu \omega' + n_{\nu-1}} = \frac{\alpha \omega' + z_{\nu-1}}{\gamma \omega' + n_{\nu-1}},$$

während nach (41)

$$(57)\quad \alpha n_{\nu-1} - \gamma z_{\nu-1} = z_\nu n_{\nu-1} - n_\nu z_{\nu-1} = (-1)^\nu = 1$$

gefunden wird. Vergleicht man aber diese Beziehung mit der vorausgesetzten Gleichung $\alpha\delta - \beta\gamma = 1$ und bedenkt, daß ebenso wie $0 < \beta < \alpha$ auch $0 < z_{\nu-1} < z_\nu$ d. i. $< \alpha$ ist, so schließt man, wie in Nr. 3 bemerkt worden ist, die Gleichheit $z_{\nu-1} = \beta$ und somit auch $n_{\nu-1} = \delta$ und solcherweise aus (56), daß der Kettenbruch

$$\lfloor \lambda, \lambda_1, \lambda_2, \ldots, \lambda_{\nu-1}, \omega' \rceil = \frac{\alpha \omega' + \beta}{\gamma \omega' + \delta} = \omega,$$

ausführlich geschrieben

$$(58)\quad \omega = \lambda + \cfrac{1}{\lambda_1 + \cfrac{1}{\lambda_2 + \cdots + \cfrac{1}{\lambda_{\nu-1} + \cfrac{1}{\omega'}}}}$$

ist.

Im zweiten Falle entwickle man $\frac{\beta}{\delta}$ in einen Kettenbruch

$$(59)\quad \frac{\beta}{\delta} = \lfloor \mu, \mu_1, \mu_2, \ldots, \mu_{\nu-1} \rceil,$$

in welchem ν ungerade sei; dann ist $z_\nu = \beta$, $n_\nu = \delta$, also

$$\beta = \mu_{\nu-1} z_{\nu-1} + z_{\nu-2}, \qquad \delta = \mu_{\nu-1} n_{\nu-1} + n_{\nu-2}$$

und

$$\frac{\beta}{\delta} = \frac{\mu_{\nu-1} z_{\nu-1} + z_{\nu-2}}{\mu_{\nu-1} n_{\nu-1} + n_{\nu-2}};$$

wenn also $\mu_{\nu-1}$ ersetzt wird durch $\mu_{\nu-1} + \omega'$, so ergibt sich der Kettenbruch

$$(60)\quad \begin{cases} \lfloor \mu, \mu_1, \mu_2, \ldots, \mu_{\nu-1} + \omega' \rceil = \dfrac{(\mu_{\nu-1} + \omega') z_{\nu-1} + z_{\nu-2}}{(\mu_{\nu-1} + \omega') n_{\nu-1} + n_{\nu-2}} \\ \qquad\qquad\qquad\qquad\qquad\quad = \dfrac{z_{\nu-1}\omega' + \beta}{n_{\nu-1}\omega' + \delta}. \end{cases}$$

Die Vergleichung der Beziehung

$$z_{\nu-1}\delta - n_{\nu-1}\beta = z_{\nu-1} n_\nu - n_{\nu-1} z_\nu = (-1)^{\nu+1} = 1$$

mit der vorausgesetzten Gleichung $\alpha\delta - \beta\gamma = 1$ ergibt aber mit Beachtung der Ungleichheiten

$$0 < \alpha < \beta, \quad 0 < z_{\nu-1} < z_\nu \text{ d. i. } < \beta$$

nach der schon vorher angezogenen Bemerkung in Nr. 3 die Gleichheit $\alpha = z_{\nu-1}$ und damit auch $\gamma = n_{\nu-1}$, mithin auch die folgende:

$$\lfloor \mu, \mu_1, \mu_2, \ldots, \mu_{\nu-1} + \omega' \rceil = \frac{\alpha\omega' + \beta}{\gamma\omega' + \delta} = \omega$$

oder ausführlich geschrieben:

$$(61)\qquad \omega = \mu + \cfrac{1}{\mu_1 + \cfrac{1}{\mu_2 + \cdots + \cfrac{1}{\mu_{\nu-1} + \omega'}}}.$$

Dies vorausgeschickt, bezeichnen wir nun mit $T(z')$ die Substitution

$$z = \frac{1}{z'}$$

und mit $S(z')$ die Substitution

$$z = z' + 1,$$

welche beide der engeren Gruppe der unimodularen Substitutionen angehören; die offenbar durch h-malige Ausführung der zweiten entstehende Substitution

$$z = z' + h$$

bezeichnen wir als $h$te Potenz von $S(z')$ durch $S^h(z')$. Hiernach entsteht augenscheinlich $\lambda_{\nu-1} + \frac{1}{\omega'}$ aus ω', wenn zuerst $T(\omega')$ und hierauf $\lambda_{\nu-1}$ mal die Substitution $S(z')$ angewandt

wird, oder durch die zusammengesetzte Substitution $S^{\lambda_\nu - 1} T(\omega')$. Nun entsteht

$$\lambda_{\nu-2} + \cfrac{1}{\lambda_{\nu-1} + \cfrac{1}{\omega'}}$$

ebenso wieder aus $\lambda_{\nu-1} + \frac{1}{\omega'}$, wenn auf letztere Größe zuerst die Substitution $T(z')$, dann $\lambda_{\nu-2}$ mal die Substitution $S(z')$ angewandt wird; jene Größe entsteht also aus ω' durch die zusammengesetzte Substitution

$$S^{\lambda_\nu - 2} T \cdot S^{\lambda_\nu - 1} T(\omega') .$$

So fortfahrend erkennt man schließlich, wenn ω durch den Kettenbruch (58) bestimmt wird, daß ω aus ω' entsteht durch die zusammengesetzte Substitution

(62a) $$S^{\lambda} T \cdot S^{\lambda_1} T \cdot S^{\lambda_2} T \ldots S^{\lambda_\nu - 1} T(\omega') ,$$

während, wenn für ω die Kettenbruchentwicklung (61) gilt, ω aus ω' durch die Substitution

(62b) $$S^{\mu} T \cdot S^{\mu_1} T \cdot S^{\mu_2} T \ldots S^{\mu_\nu - 1} (\omega')$$

hervorgebracht wird. Je nachdem also die lineare Substitution

$$\omega = \frac{\alpha\,\omega' + \beta}{\gamma\,\omega' + \delta}$$

von der angegebenen Art zur ersten oder zur zweiten der bezeichneten beiden Kategorien gehört, wird sie nach der Formel (62a) oder (62b) durch die beiden fundamentalen Substitutionen $S(z')$, $T(z')$ erzeugt.

Bedenkt man, daß die linearen Substitutionen (50) und die Transformationen (48) eindeutig einander zugeordnet sind, und daß in dieser Weise den fundamentalen Substitutionen T, S die beiden Transformationen

(63a) $$x = y', \qquad y = x'$$

und

(63b) $$x = x' + y', \qquad y = y'$$

resp. entsprechen, beachtet man ferner, daß durch Zusammen-

setzung der den Substitutionen (50), (51) entsprechenden Transformationen

$$x = \alpha x' + \beta y', \qquad y = \gamma x' + \delta y'$$
$$x' = \alpha' x'' + \beta' y'', \quad y' = \gamma' x'' + \delta' y''$$

augenscheinlich die Transformation

$$x = \alpha'' x'' + \beta'' y'', \quad y = \gamma'' x'' + \delta'' y''$$

hervorgeht, welche der aus den Substitutionen (50), (51) zusammengesetzten Substitution (52) entspricht, so läßt sich das erhaltene Resultat auch folgendermaßen aussprechen:

Jede Transformation (48), deren Koeffizienten positive, der Bedingung $\alpha\delta - \beta\gamma = 1$ genügende ganze Zahlen sind, kann aus den beiden fundamentalen Transformationen (63a), (63b) zusammengesetzt werden.

13. Wenn eine Zahl ω mit einer anderen Zahl ω' durch eine Gleichung (50) verbunden ist, in welcher die Koeffizienten $\alpha, \beta, \gamma, \delta$ der Bedingung

(64) $$\alpha\delta - \beta\gamma = \pm 1$$

genügende ganze Zahlen sind, so wird ω äquivalent mit ω' genannt. Aus der Gleichung (50) ergibt sich aber umgekehrt

$$\omega' = \frac{-\delta\omega + \beta}{\gamma\omega - \alpha},$$

wobei

(65) $$(-\delta)\cdot(-\alpha) - \beta\gamma = \pm 1$$

ist, also eine völlig entsprechende Beziehung zwischen ω' und ω, und somit ist dann auch ω' äquivalent mit ω. Wegen dieser Gegenseitigkeit der Beziehung werden zwei so verbundene Zahlen ω, ω' als zwei miteinander äquivalente Zahlen bezeichnet.

Hiernach erkennt man nun aus Nr. 11 sogleich die Tatsache, daß zwei Zahlen, welche derselben dritten Zahl äquivalent sind, es auch unter sich sein müssen. Denn, ist ω' äquivalent sowohl mit ω als auch mit ω'', so besteht, da dann auch ω äquivalent ist mit ω', eine Beziehung (50) und ebenso auch eine Beziehung (51), in denen resp.

$$\alpha\delta - \beta\gamma = \pm 1, \quad \alpha'\delta' - \beta'\gamma' = \pm 1$$

ist. Daraus folgt aber nach Nr. 11 die Beziehung (52) zugleich mit der Gleichung (54), der zufolge also

$$\alpha'' \delta'' - \beta'' \gamma'' = \pm 1$$

sein wird; demnach sind auch ω, ω'' einander äquivalent.

Man unterscheidet eigentliche und uneigentliche Äquivalenz, je nachdem in der Bedingungsgleichung (64) das obere oder das untere Vorzeichen gilt. Da in der Gleichung (65) dasselbe Vorzeichen gilt wie in (64), so ist die Äquivalenz von ω mit ω' stets von gleicher Art, wie diejenige von ω' mit ω. Ferner ersieht man aus der Gleichung (54), daß die Äquivalenz der beiden Zahlen ω, ω'' die eigentliche oder uneigentliche sein wird, je nachdem die Äquivalenz zwischen ω', ω und diejenige von ω', ω'' von gleicher oder von verschiedener Art sind. Insbesondere werden also zwei Zahlen ω, ω'', welche ein und derselben dritten Zahl ω' eigentlich äquivalent sind, auch untereinander eigentlich äquivalent sein.

Denkt man sich nun sämtliche reellen, rationalen oder irrationalen Werte, so wird man auf Grund des eben Bewiesenen ihre Gesamtheit in Klassen verteilen können, indem man immer in ein- und dieselbe Klasse alle untereinander äquivalenten Zahlen zusammenfaßt, so daß Zahlen verschiedener Klassen nicht äquivalent sein können. Spezieller noch lassen sich die Zahlen jener Gesamtheit dem zuletzt Bemerkten zufolge in engere Klassen von eigentlich äquivalenten Zahlen verteilen, wodurch dann offenbar die Menge der Klassen sich verdoppelt.

Da zwei entgegengesetzte Zahlen ω und $\omega' = -\omega$ einander stets (und zwar uneigentlich) äquivalent sind, indem

$$\omega = \frac{-1 \cdot \omega' + 0}{0 \cdot \omega' + 1}$$

gesetzt werden kann, beschränken wir uns auf die Betrachtung positiver Zahlen. Hier erkennt man leicht, daß alle rationalen Zahlen dieser Art zu einer einzigen Klasse gehören. Sind nämlich $\frac{r}{s}, \frac{r'}{s'}$ zwei positive rationale Zahlen, die in reduzierter Gestalt gedacht werden, so daß r, s und r', s' zwei

Paare teilerfremder Zahlen bedeuten, so lassen sich, wie wir wissen, zwei ganze Zahlen a, b so bestimmen, daß

$$ar' - bs' = 1$$

wird; setzt man dann

$$\alpha = ar - s'z, \quad \beta = -br + r'z, \quad \gamma = as - s'u, \quad \delta = -bs + r'u,$$

wo z, u ganze Zahlen bezeichnen, so findet sich

$$\alpha r' + \beta s' = r, \quad \gamma r' + \delta s' = s,$$

während

$$\alpha\delta - \beta\gamma = (ar' - bs')\cdot(ru - sz) = ru - sz$$

ist und folglich durch passende Wahl der ganzen Zahlen z, u gleich ± 1 gemacht werden kann. Dann ergibt sich aber

$$\frac{r}{s} = \frac{\alpha \cdot \frac{r'}{s'} + \beta}{\gamma \cdot \frac{r'}{s'} + \delta}$$

und $\alpha\delta - \beta\gamma = \pm 1$, d. h. die Äquivalenz der Zahlen $\frac{r}{s}, \frac{r'}{s'}$, wie behauptet. Alle positiven rationalen Zahlen, und daher dem vorauf Bemerkten zufolge alle rationalen Zahlen überhaupt gehören also derselben Klasse an; zudem ist offenbar zugleich mit ω' auch jede durch (50) mit ω' verbundene, d. h. ihr äquivalente Zahl ω rational, in jener Klasse also auch nur die rationalen Zahlen enthalten.

14. Bedeuten dagegen ω, ω' zwei positive aber irrationale Werte, so fragt es sich, woran man ihre Äquivalenz erkennen kann. In dieser Hinsicht gilt ein Satz, dessen wir später bedürfen werden, die Kettenbruchentwicklungen äquivalenter Zahlen betreffend. Auch positive Irrationalzahlen gestatten solche Entwicklungen, die sich von denjenigen für rationale Zahlen nur darin unterscheiden, daß sie unendlich sind. In der Tat, ist ω eine positive Irrationelle, so kann man, unter α die größte in ihr enthaltene ganze Zahl verstehend,

(66) $$\omega = 1 \cdot \alpha + b_1$$



setzen, worin b_1 positiv und kleiner als 1, aber irrational ist; desgleichen nun

$$(66)\qquad \begin{cases} 1 = b_1 \cdot \alpha_1 + b_2 \\ b_1 = b_2 \cdot \alpha_2 + b_3 \\ b_2 = b_3 \cdot \alpha_3 + b_4 \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \end{cases}$$

ganz in derselben Weise, wie für rationale Zahlen, nur daß die Reste $b_1, b_2, b_3, \ldots$ sämtlich irrational ausfallen und deshalb der Prozeß niemals ein Ende nimmt. So findet sich dann für ω eine unendlich fortlaufende Kettenbruchentwicklung

$$(67)\qquad \omega = \lfloor \alpha, \alpha_1, \alpha_2, \alpha_3, \alpha_4, \ldots \rceil;$$

bricht man aber die Reihe der Gleichungen (66) an einer endlichen Stelle etwa mit der Gleichung

$$b_{i-1} = \alpha_i b_i + b_{i+1}$$

ab, so nimmt jene unendliche Entwicklung die Gestalt eines endlichen Kettenbruchs an:

$$(68)\qquad \omega = \left\lfloor \alpha, \alpha_1, \alpha_2, \ldots, \alpha_i, \frac{b_i}{b_{i+1}} \right\rceil,$$

in welchem jedoch der sogenannte Schlußnenner, d. i. der letzte Teilnenner $\frac{b_i}{b_{i+1}}$ keine positive ganze Zahl, sondern eine positive Irrationalzahl ist.

Setzt man $\frac{b_i}{b_{i+1}} = \omega_i$, so ist, ausführlich geschrieben,

$$\omega = \alpha + \cfrac{1}{\alpha_1 + \cdots + \cfrac{1}{\alpha_i + \cfrac{1}{\omega_i}}}$$

und $\omega_i = \alpha_{i+1} + \frac{b_{i+2}}{b_{i+1}}$, also $\alpha_{i+1} < \omega_i$. Nun vermehrt man offenbar den Wert eines Kettenbruches, wenn man einen der Teilnenner ungerader Ordnung $\alpha_1, \alpha_3, \alpha_5, \ldots$ verringert, und vermindert ihn, wenn man im Gegenteil einen der Teilnenner gerader Ordnung $\alpha_2, \alpha_4, \ldots$ verringert. Hieraus folgt, daß ω zwischen den beiden endlichen Kettenbrüchen

$$\lfloor \alpha, \alpha_1, \alpha_2, \ldots, \alpha_i \rceil \quad \text{und} \quad \lfloor \alpha, \alpha_1, \alpha_2, \ldots, \alpha_i, \alpha_{i+1} \rceil$$

d. h. zwischen den beiden aufeinanderfolgenden Näherungsbrüchen $\frac{z_{i+1}}{n_{i+1}}$ und $\frac{z_{i+2}}{n_{i+2}}$ enthalten bleibt, wie groß i auch gewählt werde; daher ist der durch den unendlichen Kettenbruch nach Nr. 9 definierte Grenzwert und die in jenen entwickelte Irrationelle ω notwendig identisch.

Der **Satz** nun, um welchen es sich handelt, sagt folgendes aus:

Damit zwei positive Irrationellen ω, ω' einander äquivalent sind, ist notwendig und hinreichend, daß ihre Kettenbruchentwicklungen einen gemeinsamen Schlußnenner haben, d. h. daß jede derselben, von einer gewissen Stelle an genommen, mit der anderen übereinstimme.

Daß dieser Umstand hinreicht, ist leicht einzusehen, denn, wenn

$$\omega = \lfloor \alpha, \alpha_1, \alpha_2, \ldots, \alpha_{k-1}, \Omega \rceil$$

$$\omega' = \lfloor \beta, \beta_1, \beta_2, \ldots, \beta_{k-1}, \Omega \rceil$$

ist, so finden sich, wenn die Näherungsbrüche des ersten Kettenbruchs mit $\frac{z_i}{n_i}$, diejenigen des zweiten mit $\frac{z'_i}{n'_i}$ bezeichnet werden, Gleichungen wie diese:

$$\omega = \frac{z_h \Omega + z_{h-1}}{n_h \Omega + n_{h-1}}$$

$$\omega' = \frac{z'_k \Omega + z'_{k-1}}{n'_k \Omega + n'_{k-1}},$$

während

$$z_h n_{h-1} - n_h z_{h-1} = \pm 1, \quad z'_k n'_{k-1} - n'_k z'_{k-1} = \pm 1$$

ist, woraus zu schließen ist, daß ω, ω' beide mit Ω und daher auch untereinander äquivalent sind.

Der gleiche Umstand ist aber für die Äquivalenz von ω, ω' auch notwendig. Besteht nämlich eine Beziehung

$$\omega = \frac{\alpha \omega' + \beta}{\gamma \omega' + \delta} \tag{69}$$

mit $\alpha\delta - \beta\gamma = \pm 1$, und ist die Kettenbruchentwicklung für ω', an irgend einer Stelle abgebrochen, diese:

$$\omega' = \lfloor \beta, \beta_1, \beta_2, \ldots, \beta_{k-1}, \Omega \rfloor,$$

so daß Ω den unendlichen Schlußteil

$$\Omega = \lfloor \beta_k, \beta_{k+1}, \beta_{k+2}, \ldots \rceil$$

d. i. einen positiven Wert bedeutet, so darf man setzen

$$\omega' = \frac{z'_k \Omega + z'_{k-1}}{n'_k \Omega + n'_{k-1}},$$

wodurch die Formel (69) in die andere

$$(70) \qquad \omega = \frac{(\alpha z'_k + \beta n'_k)\,\Omega + \alpha z'_{k-1} + \beta n'_{k-1}}{(\gamma z'_k + \delta n'_k)\,\Omega + \gamma z'_{k-1} + \delta n'_{k-1}}$$

übergeht. Da nun

$$\frac{\alpha z'_k + \beta n'_k}{\alpha z'_{k-1} + \beta n'_{k-1}} = \frac{n'_k}{n'_{k-1}} \cdot \frac{\frac{z'_k}{n'_k} + \frac{\beta}{\alpha}}{\frac{z'_{k-1}}{n'_{k-1}} + \frac{\beta}{\alpha}}$$

ist, und mit unendlich wachsendem Index k die Näherungsbrüche $\frac{z'_{k-1}}{n'_{k-1}}, \frac{z'_k}{n'_k}$ sich beide dem Grenzwerte des unendlichen Kettenbruchs, d. i. dem Werte ω', unendlich annähern, so nähert sich der zweite Faktor zur Rechten in voriger Gleichung dem Werte 1, während der erste positiv und größer als 1 bleibt. Für einen hinreichend großen Wert von k ist also

$$(71) \qquad \frac{\alpha z'_k + \beta n'_k}{\alpha z'_{k-1} + \beta n'_{k-1}}$$

ein positiver unechter Bruch, der, in den kleinsten positiven Zahlen ausgedrückt, $\frac{A}{B}$ genannt werde. Ganz ebenso findet sich für ein gleichfalls hinreichend großes k, das dem ersten gleich gewählt werden darf,

$$(72) \qquad \frac{\gamma z'_k + \delta n'_k}{\gamma z'_{k-1} + \delta n'_{k-1}}$$

als ein positiver unechter Bruch, dessen Ausdruck in den kleinsten positiven Zahlen $\frac{C}{D}$ sei. Der Index k kann überdies (Nr. 10) so gewählt werden, daß in der Beziehung

$$z'_k n'_{k-1} - n'_k z'_{k-1} = \pm 1$$

dasselbe Vorzeichen gelte, wie in der Gleichung $\alpha\delta - \beta\gamma = \pm 1$. Da ferner dann

$$(73)\qquad \begin{cases} (\alpha z'_k + \beta n'_k)(\gamma z'_{k-1} + \delta n'_{k-1}) \\ - (\alpha z'_{k-1} + \beta n'_{k-1})(\gamma z'_k + \delta n'_k) \\ = (\alpha\delta - \beta\gamma)(z'_k n'_{k-1} - n'_k z'_{k-1}) = 1 \end{cases}$$

ist, so sind Zähler und Nenner in jedem der Brüche (71), (72) teilerfremd und man schließt demnach

$$\alpha z'_k + \beta n'_k = \varepsilon A, \qquad \alpha z'_{k-1} + \beta n'_{k-1} = \varepsilon B$$
$$\gamma z'_k + \delta n'_k = \varepsilon' C, \qquad \gamma z'_{k-1} + \delta n'_{k-1} = \varepsilon' D,$$

wo $\varepsilon, \varepsilon'$ Einheiten bedeuten; aus (70) folgt also

$$\omega = \frac{\varepsilon}{\varepsilon'} \cdot \frac{A\Omega + B}{C\Omega + D};$$

da aber ω als positiv vorausgesetzt ist, müssen $\varepsilon, \varepsilon'$ dieselbe Einheit bezeichnen und demnach wird

$$\omega = \frac{A\Omega + B}{C\Omega + D},$$

während A, B, C, D positive ganze Zahlen bedeuten, für welche die Bedingungen

$$A > B, \qquad C > D$$

und wegen (73) die Gleichung

$$(74)\qquad AD - BC = 1$$

erfüllt sind.

Dies vorausgeschickt, denke man sich den Bruch $\frac{A}{C}$ in einen gewöhnlichen Kettenbruch entwickelt:

$$\frac{A}{C} = \lfloor \alpha, \alpha_1, \alpha_2, \ldots, \alpha_{k-1} \rceil,$$

nenne $\frac{A'}{C'}$ seinen vorletzten Näherungsbruch und wähle dabei die Anzahl der Teilnenner so, daß in der Gleichung

$$AC' - A'C = \pm 1$$

das obere Vorzeichen gelte, was nach Nr. 10 zu erreichen möglich ist. Da auch in dieser Gleichung A, C, A', C' positive ganze Zahlen sind, für welche

$$A > A', \qquad C > C'$$

ist, erschließt man auf Grund der in Nr. 3 gemachten Bemerkung die Gleichheiten

$$A' = B, \quad C' = D,$$

und der Kettenbruch

$$\lfloor \alpha, \alpha_1, \alpha_2, \ldots, \alpha_{h-1}, \Omega \rceil$$

wird mit

$$\frac{A\Omega + A'}{C\Omega + C'} = \frac{A\Omega + B}{C\Omega + D}$$

d. h. mit ω identisch sein. Die beiden durch die Beziehung (69) und die Bedingung $\alpha\delta - \beta\gamma = \pm 1$ verbundenen, d. h. einander äquivalenten Irrationellen ω, ω' haben also in der Tat, wie zu beweisen war, Kettenbruchentwicklungen mit demselben Schlußnenner Ω.

Fünftes Kapitel.

Die quadratischen Formen.

1. Die Aufgabe, die unbestimmte Gleichung ersten Grades

$$ax + by = m,$$

in welcher m und a, b ganze Zahlen bedeuten, aufzulösen, ist schon nebst anderen Gleichungen derselben Art von *Diophant* behandelt worden und heißt deshalb eine *Diophant*ische Gleichung und die Theorie dieser und ähnlicher Gleichungen *Diophant*ische Analysis. Nachdem aber das Problem für Gleichungen ersten Grades erledigt worden, war es natürlich, unbestimmte Gleichungen höheren, zunächst des zweiten Grades zu behandeln. Die allgemeine Aufgabe dieser Art ließ sich, solange nur zwei Unbestimmte ins Auge gefaßt wurden, auf die speziellere zurückführen, die Gleichung

(1) $$ax^2 + bxy + cy^2 = m,$$

wo m und a, b, c ganze Zahlen bedeuten, in ganzen Zahlen x, y zu lösen, oder, wie man zu sagen pflegt, die Zahl m in der Form

(2) $$f(x, y) = ax^2 + bxy + cy^2$$

mittels ganzzahliger Werte der Unbestimmten x, y darzustellen. Jeden Ausdruck dieser Art nennt man eine quadratische, insbesondere, da nur zwei Unbestimmte auftreten, eine binäre quadratische Form. Schon waren über derartige Formen mancherlei einzelne Sätze gewonnen worden, als im 18. Jahrhundert *Euler* und neben ihm vornehmlich *Lagrange* und *Legendre* ihre Untersuchung eingehender aufnahmen und bedeutend förderten. Doch war es erst *Gauß*, welcher in seinen Disquis. arithmet. (1801) ihre Theorie von Grund aus in strenger Systematik und bewundernswerter Vollständigkeit entwickelte. Seitdem ist man freilich in mehrfacher Hinsicht noch erheblich fortgeschritten. Das *Gauß*sche Gebäude der Lehre von den quadratischen Formen ruht wesentlich auf den algebraischen Eigenschaften ihres Ausdrucks. Neuerdings aber hat man nicht nur geometrische Deutungen desselben, wie deren eine schon von *Gauß* selbst angegeben worden, benutzt, um die formell rechnerischen *Gauß*schen Methoden durch anschauliche zu ersetzen, sondern man hat auch den eigentlich arithmetischen Kern der Lehre zu erfassen und herauszuschälen gewußt, indem man an die Stelle der quadratischen Formen den sogenannten quadratischen Zahlenkörper gesetzt und so eine Arithmetik geschaffen hat, die als eine der gewöhnlichen analoge, aber höhere Zahlentheorie zu betrachten ist. Es ist unsere Absicht, die Lehre von den quadratischen Formen hier so darzustellen, daß dabei den angedeuteten verschiedenen Auffassungen zugleich gebührende Rechnung getragen werde und ein einheitliches Ganzes entstehe, das durch die so gewonnene vielseitige Beleuchtung möglichst klare und tiefe Einsicht in das Wesen der Lehre gewährt.

2. Wir gehen aus von den Grundlagen der *Gauß*schen Theorie. Deren sind wesentlich zwei.

Erstens: der Ausdruck (2) läßt sich schreiben wie folgt:

$$f(x, y) = \left(ax + \frac{b}{2}y\right)x + \left(\frac{b}{2}x + cy\right)y$$

oder, wenn

$$ax + \frac{b}{2}y = X, \quad \frac{b}{2}x + cy = Y$$

gesetzt wird,

$$f(x, y) = Xx + Yy. \tag{3}$$

Ebenso wird für andere Werte x', y' der Unbestimmten

(4) $$f(x', y') = X'x' + Y'y'$$

sein, wenn

$$a x' + \frac{b}{2} y' = X', \quad \frac{b}{2} x' + c y' = Y'$$

gesetzt wird. Hiernach findet man durch leichte Rechnung

(5) $$\begin{cases} (Xx + Yy)(X'x' + Y'y') - (Xx' + Yy')(X'x + Y'y) \\ \qquad = (XY' - X'Y) \cdot (xy' - x'y) \end{cases}$$

und

(6) $$XY' - X'Y = \left(ac - \frac{b^2}{4}\right) \cdot (xy' - x'y).$$

Wird letzterer Ausdruck in die voraufgehende Gleichung eingesetzt und neben den Gleichungen (3) und (4) diese andere:

$$Xx' + Yy' = \left(ax + \frac{b}{2} y\right) x' + \left(\frac{b}{2} x + cy\right) y' = X'x + Y'y$$

beachtet, so ergibt sich nachstehende Formel:

(7) $$\begin{cases} f(x, y) \cdot f(x', y') = \left[\left(ax + \frac{b}{2} y\right) x' + \left(\frac{b}{2} x + cy\right) y'\right]^2 \\ \qquad - \frac{1}{4} (b^2 - 4ac) \cdot (xy' - x'y)^2. \end{cases}$$

Diese Identität ist eine der gedachten Grundlagen. Man sieht hier eine aus den Koeffizienten a, b, c der quadratischen Form gebildete Zahl $b^2 - 4ac$ erscheinen, welche für die ganze Theorie derselben geradezu bestimmende Bedeutung hat und daher von *Gauß* als Determinante der Form bezeichnet worden ist*); wir nennen sie lieber ihre Diskriminante und setzen dafür kurz das Zeichen D, also:

(8) $$D = b^2 - 4ac,$$

so daß die Grundformel (7) auch folgendermaßen geschrieben werden kann:

(9) $$\begin{cases} 4 \cdot f(x, y) f(x', y') = [(2ax + by) x' + (bx + 2cy) y']^2 \\ \qquad - D \cdot (xy' - x'y)^2. \end{cases}$$

*) In Wahrheit tritt dafür bei *Gauß*, welcher die quadratischen Formen in der Gestalt $ax^2 + 2bxy + cy^2$ behandelt, nämlich den mittleren Koeffizienten stets als gerade voraussetzt, die Zahl $b^2 - ac$ auf.

Gibt man in dieser Identität den Unbestimmten x', y' einmal die Werte 1, 0, ein zweites Mal die Werte 0, 1, so gehen daraus die Werte

$$(10)\qquad f(1,\,0) = a\,,\quad f(0,\,1) = c$$

und die beiden Formeln

$$(11)\qquad \begin{cases} 4a\cdot f(x,\,y) = (2ax + by)^2 - Dy^2 \\ 4c\cdot f(x,\,y) = (bx + 2cy)^2 - Dx^2 \end{cases}$$

hervor.

Die Bedeutung der Diskriminante zeigt sich nun sogleich darin, daß die quadratischen Formen von wesentlich anderer Beschaffenheit sind, je nachdem jene positiv, Null oder negativ ist. Ist $D = 0$, so zeigen die Formeln (11), daß die quadratische Form im Grunde das Quadrat einer Linearform ist, indem sie einem solchen gleich wird, wenn sie mit dem vierfachen ersten oder letzten Koeffizienten multipliziert wird. Aus diesem Grunde werden wir in der Folge von dem Falle einer verschwindenden Diskriminante absehen.

Ist D negativ, so zeigen die Formeln (11), daß deren rechte Seiten für alle ganzzahligen (sogar für alle reellen) Werte der Unbestimmten, wenn sie nicht zugleich Null sind, einen positiven Wert, also die Form $f(x,\,y)$ das gleiche Vorzeichen hat wie a und c, welche beiden Koeffizienten dann gleiches Vorzeichen haben müssen. Sind sie beide positiv, so lassen sich durch die Form $f(x,\,y)$ nur positive, sind sie beide negativ, nur negative Zahlen darstellen. Daher heißt dann die Form selbst resp. eine positive oder eine negative und, beide Fälle vereinigt, eine bestimmte Form (forma definita). Es genügt, in der Folge nur positive Formen zu betrachten.

Ist dagegen D positiv, so heißt die Form eine unbestimmte (forma indefinita), weil alsdann Zahlen beiderlei Vorzeichens durch sie darstellbar sind. In der Tat, entweder sind beide Zahlen a, c gleich Null, also $f(x,\,y) = bxy$, dann erhält die Form das gleiche oder das entgegengesetzte Vorzeichen wie b, je nachdem x, y mit gleichem oder entgegengesetztem Vorzeichen gewählt werden; oder es ist etwa a nicht Null, dann wird die rechte Seite der ersten Formel (11) positiv, wenn $y = 0$ gewählt wird, dagegen negativ, wenn

die ganzen Zahlen x, y, was stets möglich ist, so gewählt werden, daß $2ax + by = 0$ wird.

3. Bei solcher Bedeutsamkeit der Diskriminante wird es geboten sein, diejenigen Formen zusammenzuhalten, welche gleiche Diskriminante haben. Wir werden daher die Diskriminante D als eine ein für allemal gegebene Zahl ansehen und die Betrachtung auf die Formen mit dieser Diskriminante D beschränken. Nicht jede Zahl aber kann Diskriminante einer quadratischen Form sein, denn, je nachdem b gerade oder ungerade, b^2 also $\equiv 0$ oder $\equiv 1 \pmod{4}$ ist, findet sich $D = b^2 - 4ac$ ebenfalls $\equiv 0$ oder $\equiv 1 \pmod{4}$, es gibt also keine quadratische Form, deren Diskriminante $\equiv 2$ oder $\equiv 3 \pmod{4}$ wäre. Genügt jedoch D der Bedingung, kongruent 0 oder 1 (mod. 4) zu sein, so gibt es unendlich viel Formen mit der Diskriminante D; denn, wählt man für b irgend eine zugleich mit D gerade resp. ungerade Zahl, so ergibt sich $b^2 \equiv D \pmod{4}$, also $\frac{b^2 - D}{4}$ als eine ganze Zahl, und jede Zerlegung derselben in zwei Faktoren a, c liefert eine quadratische Form $ax^2 + bxy + cy^2$ oder, wie wir bisweilen abkürzend sagen wollen, eine Form (a, b, c), deren Diskriminante $b^2 - 4ac = D$ ist. Um unsere Untersuchungen zu vereinfachen, wollen wir indessen die Diskriminante selbst möglichst einfach voraussetzen und uns auf sogenannte Stammdiskriminanten beschränken. Wir verstehen darunter entweder eine Diskriminante $D \equiv 1 \pmod{4}$, welche durch kein Quadrat teilbar ist, oder falls $D \equiv 0 \pmod{4}$ ist, eine Diskriminante, für welche $\frac{D}{4}$ durch kein Quadrat aufgeht, auch selbst keine Diskriminante mehr sein kann und somit (mod. 4) einen der Reste 2 oder 3 läßt. Bezeichnet also d eine durch kein Quadrat teilbare Zahl, so ist entweder

$$(12\text{a}) \qquad D = d \quad \text{und} \quad d \equiv 1 \pmod{4}$$

oder

$$(12\text{b}) \qquad D = 4d \quad \text{und} \quad d \equiv 2, 3 \pmod{4}$$

vorauszusetzen. Bei solcher Voraussetzung können die drei Koeffizienten a, b, c der Form keinen gemeinsamen Teiler haben; denn sonst erhielte, wenn $D = b^2 - 4ac = d$ ist, d

einen quadratischen Teiler; wenn aber $D = b^2 - 4ac = 4d$, also b gerade, etwa $b = 2\beta$ und $\beta^2 - ac = d$ ist, erhielte wieder d einen quadratischen Teiler, falls ein gemeinsamer Primteiler von a, b, c auch ein solcher von a, β, c ist, oder d würde $\equiv 1$ (mod. 4), falls er gleich 2, β aber ungerade ist — gegen die Voraussetzung. Quadratische Formen, deren Koeffizienten ohne gemeinsamen Teiler sind, werden primitiv genannt; die Beschränkung auf Stammdiskriminanten bedingt also zugleich diejenige auf primitive Formen.

4. Fragt man nun nach der Darstellbarkeit einer Zahl m durch die (primitive) Form (a, b, c), so hat man zunächst zwischen Darstellungen zu unterscheiden, bei denen die darstellenden Zahlen, d. i. die Werte der Unbestimmten, durch welche die Gleichung (1) erfüllt wird, einen gemeinsamen Teiler haben, und solchen, bei denen sie teilerfremd sind. Wäre α, γ eine Darstellung von m, so daß die Gleichung

$$a\alpha^2 + b\alpha\gamma + c\gamma^2 = m \tag{13}$$

statthätte, und hätten α, γ den größten gemeinsamen Teiler $\tau > 1$, so daß $\alpha = \tau\alpha'$, $\gamma = \tau\gamma'$ und α', γ' teilerfremde Zahlen wären, so müßte offenbar m den quadratischen Teiler τ^2 haben, und wenn man mit diesem die Gleichung (13) dividierte, erhielte man

$$a\alpha'^2 + b\alpha'\gamma' + c\gamma'^2 = \frac{m}{\tau^2}, \tag{14}$$

d. i. eine Darstellung von $\frac{m}{\tau^2}$, bei welcher die darstellenden Zahlen α', γ' teilerfremd sind. Solche Darstellungen wollen wir kurz eigentliche Darstellungen nennen. Aus dem Gesagten ersieht man, daß die allgemeine Aufgabe, die Darstellungen einer Zahl durch eine quadratische Form zu ermitteln, auf die bestimmtere zurückkommt, die eigentlichen Darstellungen einer Zahl zu finden; auf sie dürfen wir fortan unsere Betrachtung beschränken; die übrigen erhält man offenbar, wenn man für jeden quadratischen Teiler τ^2 jener Zahl m die eigentlichen Darstellungen α', γ' von $\frac{m}{\tau^2}$ mit τ multipliziert.

Was aber die eigentlichen Darstellungen von m betrifft, so liefert darüber die Grundformel (9) sogleich einen fundamentalen Satz. Bezeichnen α, γ eine eigentliche Darstellung

von m durch (a, b, c), so sind α, γ teilerfremd und daher können zwei Zahlen β, δ so gewählt werden, daß

$$\alpha\delta - \beta\gamma = 1 \tag{15}$$

wird. Setzt man dann für $x, y; x', y'$ in (9) resp. $\alpha, \gamma; \beta, \delta$, so ergibt sie die Beziehung:

$$4\cdot f(\alpha, \gamma) f(\beta, \delta) = [(2a\alpha + b\gamma)\beta + (b\alpha + 2c\gamma)\delta]^2 - D. \tag{16}$$

Hierin ist nach Voraussetzung

$$f(\alpha, \gamma) = a\alpha^2 + b\alpha\gamma + c\gamma^2 = m; \tag{17a}$$

setzt man ferner

$$\begin{cases} f(\beta, \delta) = a\beta^2 + b\beta\delta + c\delta^2 = n \\ (2a\alpha + b\gamma)\beta + (b\alpha + 2c\gamma)\delta = r, \end{cases} \tag{17b}$$

so nimmt die Gleichung (16) die Form an

$$4mn = r^2 - D \tag{18}$$

und lehrt, daß

$$r^2 \equiv D \pmod{4m}, \tag{19}$$

d. h. nach der in Kap. 3, Nr. 1 eingeführten Ausdrucksweise, daß D quadratischer Rest sein muß von $4m$. Da in diesem Resultate von der Form (a, b, c), durch welche die Darstellung von m gedacht wird, nur ihre Diskriminante auftritt, so haben wir eine notwendige Bedingung für die Darstellbarkeit der Zahl m nicht sowohl durch die besondere Form (a, b, c), als vielmehr durch irgend eine Form mit der Diskriminante D gefunden.

Ist diese notwendige Bedingung erfüllt, so folgt daraus zwar nicht die eigentliche Darstellbarkeit der Zahl m durch die besondere Form (a, b, c) mit der Diskriminante D, wohl aber, daß es unendlich viel Formen mit dieser Diskriminante gibt, durch welche m eigentlich dargestellt werden kann. In der Tat, ist D quadratischer Rest von $4m$, so ist die Kongruenz

$$z^2 \equiv D \pmod{4m} \tag{20}$$

auflösbar und jeder Lösung r derselben entspricht eine ganze Zahl $n = \dfrac{r^2 - D}{4m}$, also eine quadratische Form $(m, r, n) = mx^2 + rxy + ny^2$ mit der Diskriminante D und dem ersten Koeffizienten m, durch welche also m mittels der

teilerfremden Zahlen $x = 1$, $y = 0$, d. h. eigentlich dargestellt wird. Ist aber r eine Lösung der Kongruenz (20), so gibt es unendlich viel Zahlen $\varrho \equiv r \pmod{4m}$, welche sie auch lösen und eine bestimmte Wurzel der Kongruenz bilden; die unendlich vielen, ihnen entsprechenden quadratischen Formen $\left(m, \varrho, \frac{\varrho^2 - D}{4m}\right)$ mit der Diskriminante D und dem ersten Koeffizienten m mögen eine Schar von Parallelformen genannt werden. Hiernach wird es so viel Scharen von Parallelformen mit der Diskriminante D und dem ersten Koeffizienten m geben, durch welche mithin m eigentlich darstellbar ist, als die Kongruenz (20) verschiedene Wurzeln besitzt.

War nun m durch die besondere Form (a, b, c) mittels der Zahlen α, γ eigentlich darstellbar, so ergab diese Darstellung nach den Gleichungen (17) bis (19) eine bestimmte Lösung r der Kongruenz (20). Dabei waren β, δ eine besondere Lösung der Gleichung (15), aus welcher alle übrigen Lösungen derselben durch die Formeln

$$\beta' = \beta + \alpha z, \qquad \delta' = \delta + \gamma z$$

gefunden werden, wenn z alle ganzzahligen Werte annimmt. Ersetzt man aber β, δ im Ausdrucke für r durch β', δ', so geht eine Gleichung

$$\varrho = (2a\alpha + b\gamma)\beta' + (b\alpha + 2c\gamma)\delta' = r + 2mz,$$

d. i., wenn z gerade gedacht wird, die Kongruenz $\varrho \equiv r \pmod{4m}$ hervor, und da auf solche Weise durch passende Wahl von z jede mit $r \pmod{4m}$ kongruente Zahl ϱ entsteht, so entspricht also allen den bezeichneten Lösungen der Gleichung (15) eine bestimmte Wurzel der Kongruenz (20) oder eine bestimmte Schar von Parallelformen mit dem ersten Koeffizienten m. Man sagt hiernach, daß jede eigentliche Darstellung von m durch eine Form mit der Diskriminante D zu einer bestimmten Wurzel der Kongruenz (20) gehöre, und bezeichnet die Gesamtheit aller eigentlichen Darstellungen von m durch jene Form, welche etwa zu derselben Kongruenzwurzel gehören, als eine Darstellungsgruppe.

5. Um diese Verhältnisse klarer zu durchschauen, dient die zweite der in Nr. 2 gemeinten Grundlagen: die

Transformation einer quadratischen Form mittels einer Substitution

(21) $$x = \alpha x' + \beta y', \qquad y = \gamma x' + \delta y',$$

deren Koeffizienten $\alpha, \beta, \gamma, \delta$ ganze Zahlen sind. Wird diese in der Form

(22) $$f(x, y) = a x^2 + b x y + c y^2$$

ausgeführt, so entsteht der Ausdruck

$$\begin{aligned} &a(\alpha x' + \beta y')^2 + b(\alpha x' + \beta y')(\gamma x' + \delta y') + c(\gamma x' + \delta y')^2 \\ &= (a\alpha^2 + b\alpha\gamma + c\gamma^2) x'^2 + (2a\alpha\beta + b(\alpha\delta + \beta\gamma) + 2c\gamma\delta) x'y' \\ &\qquad + (a\beta^2 + b\beta\delta + c\delta^2) y'^2, \end{aligned}$$

d. i. die quadratische Form

(23) $$f'(x', y') = a' x'^2 + b' x' y' + c' y'^2,$$

deren Koeffizienten durch die Gleichungen

(24) $$\begin{cases} a' = a\alpha^2 + b\alpha\gamma + c\gamma^2 = f(\alpha, \gamma) \\ b' = (2a\alpha + b\gamma)\beta + (b\alpha + 2c\gamma)\delta \\ c' = a\beta^2 + b\beta\delta + c\delta^2 = f(\beta, \delta) \end{cases}$$

bestimmt sind. Durch die Transformation (21) geht also die quadratische Form $f(x, y)$ in eine andere quadratische Form $f'(x', y')$ über. Ersetzt man aber $x, y; x', y'$ in der Grundformel (7) durch $\alpha, \gamma; \beta, \delta$ resp., so liefert sie bei Beachtung der vorstehenden Gleichungen die Beziehung

$$4a'c' - b'^2 = (4ac - b^2) \cdot (\alpha\delta - \beta\gamma)^2,$$

d. h. wenn die Diskriminante der neuen Form mit D' bezeichnet wird, zwischen den Diskriminanten der ursprünglichen und der neuen Form die Beziehung

(25) $$D' = D \cdot (\alpha\delta - \beta\gamma)^2.$$

Die Diskriminanten beider Formen werden also dann, aber auch nur dann einander gleich, wenn die ganzzahligen Koeffizienten der Transformationsgleichungen (21) die Bedingung erfüllen

(26) $$\alpha\delta - \beta\gamma = \pm 1.$$

In dieser Voraussetzung entsprechen aber auf Grund der Gleichungen (21) ganzzahligen Werten der Unbestimmten

x', y' stets auch solche der Unbestimmten x, y, und umgekehrt, und da vermittels jener Gleichungen die Identität $f(x, y) = f'(x', y')$ besteht, so ersieht man, daß die Gesamtheit der Zahlen, welche durch $f(x, y)$ darstellbar sind, mit der Gesamtheit der durch $f'(x', y')$ darstellbaren Zahlen übereinstimmen muß. Dies gilt auch insbesondere für die Gesamtheit der durch die Formen eigentlich darstellbaren Zahlen, denn jeder gemeinsame Teiler von x', y' ist den Gleichungen (21) zufolge auch ein solcher von x, y, und nach den aus ihrer Auflösung folgenden Gleichungen

$$(27) \qquad x' = \delta x - \beta y, \quad y' = -\gamma x + \alpha y$$

auch umgekehrt, und somit müssen x', y' teilerfremd sein, wenn es x, y sind, und umgekehrt. Aus solchem Grunde nennen wir die Form $f'(x', y')$, wenn sie aus der Form $f(x, y)$ durch eine unimodulare d. i. der Bedingung (26) genügende Transformation (21) entsteht, äquivalent mit $f(x, y)$. Da alsdann $f'(x', y')$ offenbar durch die aufgelösten Gleichungen (21), d. i. durch die Transformation (27), deren Koeffizienten der mit (26) analogen Bedingung

$$(28) \qquad \delta \cdot \alpha - (-\beta)(-\gamma) = \pm 1$$

genügen, wieder in $f(x, y)$ zurückverwandelt wird, ist dann $f(x, y)$ auch äquivalent mit $f'(x', y')$ und somit beide Formen einander äquivalent.

Äquivalente Formen haben also gleiche Diskriminanten, ein Satz, der aber nicht umgekehrt werden darf, und stellen genau die gleichen Zahlen (eigentlich) dar. Man unterscheidet eigentliche und uneigentliche Äquivalenz, je nachdem in der Bedingungsgleichung (26) für die Koeffizienten der Transformation das obere oder das untere Vorzeichen gilt.

Hier besteht ferner der Satz, daß zwei Formen, welche mit derselben dritten Form (eigentlich) äquivalent sind, es auch untereinander sind. In der Tat, ist $f(x, y)$ äquivalent einerseits mit $f'(x', y')$, andererseits mit $f''(x'', y'')$, und bezeichnen

$$x = \alpha x' + \beta y', \quad y = \gamma x' + \delta y', \quad \alpha\delta - \beta\gamma = \pm 1$$

und

$$x = \lambda x'' + \mu y'', \quad y = \nu x'' + \varrho y'', \quad \lambda\varrho - \mu\nu = \pm 1$$

die Transformationen, welche $f(x, y)$ in jene Formen verwandeln, so besteht auf Grund dieser Gleichungen die Identität

$$f(x, y) = f'(x', y') = f''(x'', y''),$$

die Gleichungen (27), welche durch Auflösung der ersteren dieser Gleichungen entstehen, nehmen aber, wenn darin für x, y die letzteren Ausdrücke substituiert werden, die Gestalt

$$x' = (\delta\lambda - \beta\nu)\, x'' + (\delta\mu - \beta\varrho)\, y'',$$
$$y' = (-\gamma\lambda + \alpha\nu)\, x'' + (-\gamma\mu + \alpha\varrho)\, y''$$

an und bezeichnen wegen $f'(x', y') = f''(x'', y'')$ eine Transformation der Form $f'(x', y')$ in die Form $f''(x'', y'')$, deren Koeffizienten durch die Beziehung

$$(\delta\lambda - \beta\nu)(-\gamma\mu + \alpha\varrho) - (\delta\mu - \beta\varrho)(-\gamma\lambda + \alpha\nu)$$
$$= (\alpha\delta - \beta\gamma)(\lambda\varrho - \mu\nu) = \pm 1$$

miteinander verbunden sind; die genannten zwei Formen sind also, wie behauptet, einander äquivalent. Zugleich ist diese Äquivalenz eine eigentliche, wenn die Äquivalenz von $f(x, y)$ mit jeder der Formen $f'(x', y')$, $f''(x'', y'')$ von gleicher Art ist, entgegengesetztenfalls eine uneigentliche.

Auf Grund dieses Satzes können jetzt sämtliche Formen mit derselben Diskriminante D in Klassen eingeteilt werden, indem man alle untereinander (eigentlich) äquivalenten Formen je in eine Klasse zusammenfaßt, derart daß Formen, welche verschiedenen Klassen angehören, einander nicht (eigentlich) äquivalent sein können. Wählt man dann aus jeder Klasse nach Belieben eine Form aus und bezeichnet diese durch

$$(29) \qquad f_1(x, y), \quad f_2(x, y), \quad f_3(x, y), \ldots,$$

so sollen letztere Formen ein Repräsentantensystem für die Klassen (eigentlich) äquivalenter Formen oder kürzer für alle Formen mit der Diskriminante D genannt werden.

6. Fragt man nun nach der Gesamtheit von Zahlen, welche überhaupt durch Formen mit der Diskriminante D (eigentlich) darstellbar sind, so genügt es offenbar, diese Gesamtheit für deren Repräsentanten (29) zu suchen, denn durch äquivalente Formen werden ja nur dieselben Zahlen (eigentlich) dargestellt. Fragen wir aber bestimmter nach den etwa vorhandenen eigentlichen Darstellungen — nur

solche wollen wir berücksichtigen — einer gegebenen Zahl m durch eine gegebene Form $f(x, y) = ax^2 + bxy + cy^2$, die als Repräsentant ihrer Klasse gewählt werden kann, so ist zunächst erforderlich, daß D quadratischer Rest von $4m$, d. h. daß die Kongruenz (20) auflösbar sei. Wäre dann α, γ eine eigentliche Darstellung von m durch die Form (a, b, c), so zeigt die Vergleichung der daraus abgeleiteten Gleichungen (17a) und (17b) mit den Formeln (24) sogleich an, daß die Form (a, b, c) durch die Substitution (21), deren Koeffizienten die Bedingung $\alpha\delta - \beta\gamma = 1$ erfüllen, in die Form

$$(30) \qquad (m, r, n) = \left(m, r, \frac{r^2 - D}{4m}\right)$$

verwandelt würde und somit dieser Form, allgemeiner jeder der Formen $\left(m, \varrho, \frac{\varrho^2 - D}{4m}\right)$, in denen $\varrho \equiv r \pmod{4m}$, d. h. der ganzen, der Kongruenzwurzel r, zu der die Darstellung gehört, entsprechenden Schar von Parallelformen äquivalent wäre, die deshalb sämtlich auch untereinander es wären. Bezeichnet man also mit $r, r', r'', \ldots$ die sämtlichen Wurzeln der Kongruenz (20) und wählt aus den ihnen entsprechenden Scharen von Parallelformen mit dem ersten Koeffizienten m je eine aus:

$$(31) \qquad \begin{cases} \left(m, r, \frac{r^2 - D}{4m}\right), \quad \left(m, r', \frac{r'^2 - D}{4m}\right), \\ \qquad \left(m, r'', \frac{r''^2 - D}{4m}\right), \ldots, \end{cases}$$

so muß die Form $f(x, y)$, wenn m eigentlich durch sie darstellbar sein soll, einer (oder mehreren) von diesen eigentlich äquivalent sein. Findet sie sich aber eigentlich äquivalent etwa mit der Form

$$\left(m, r, \frac{r^2 - D}{4m}\right) = (m, r, n),$$

d. h. läßt sich eine Substitution (21) mit der Bedingung $\alpha\delta - \beta\gamma = 1$ ermitteln, durch welche sie in die letztere Form übergeht, so ergibt die erste der nach Nr. 5 hieraus folgenden Gleichungen

$$m = a\alpha^2 + b\alpha\gamma + c\gamma^2$$
$$r = (2a\alpha + b\gamma)\beta + (b\alpha + 2c\gamma)\delta$$
$$n = a\beta^2 + b\beta\delta + c\delta^2$$

in der Tat eine eigentliche Darstellung α, γ der Zahl m durch die Form (a, b, c), und die Vergleichung vorstehender Gleichungen mit den obigen (17a) und (17b) läßt genauer erkennen, daß diese Darstellung zur Kongruenzwurzel r gehört, der die Form (m, r, n) entspricht.

Auf solche Weise kommt die Aufgabe, eine eigentliche Darstellung der gegebenen Zahl m durch eine gegebene quadratische Form (a, b, c) zu finden, auf die andere Aufgabe zurück, über die eigentliche Äquivalenz zweier Formen zu entscheiden, eine Entscheidung, die bejahendenfalls die Ermittlung einer Transformation der einen Form in die andere mit sich bringt. Indem wir daher die weitere Aufgabe: die sämtlichen eigentlichen Darstellungen von m durch jene Form zu finden, auf eine spätere Stelle verschieben, stellen wir das Problem der Äquivalenz in den Vordergrund und wollen nun zunächst dies Problem von anderen Seiten beleuchten.

7. Das erste sei eine geometrische Deutung der quadratischen Formen und ihrer Äquivalenz. Dabei müssen wir Formen mit positiver Diskriminante von denen mit negativer trennen und beginnen mit der Erörterung der letzteren.

Um die Form

(32) $$f(x, y) = ax^2 + bxy + cy^2$$

geometrisch zu interpretieren, bemerke man zunächst, daß wegen der Voraussetzung

$$D = b^2 - 4ac < 0$$

der Bruch $\frac{b}{2\sqrt{ac}}$ reell und numerisch kleiner ist als 1, daß also ein Winkel φ angebbar ist, für welchen

(33) $$\cos\varphi = \frac{b}{2\sqrt{ac}}$$

ist; da wir zudem nur positive Formen behandeln, sind a, c positiv, also auch $\sqrt{a}$, $\sqrt{c}$ reell. Nun denke man sich (Fig. 3)

auf einer Geraden $X'OX$ von O aus nach beiden Seiten die Strecke $OA = \sqrt{a}$ beliebig oft aufgetragen, ziehe durch O eine Gerade $L'OL$ unter dem Neigungswinkel φ gegen die erstere Gerade und trage auf ihr von O aus nach beiden Seiten die Strecke $OC = \sqrt{c}$ beliebig oft auf und ziehe endlich

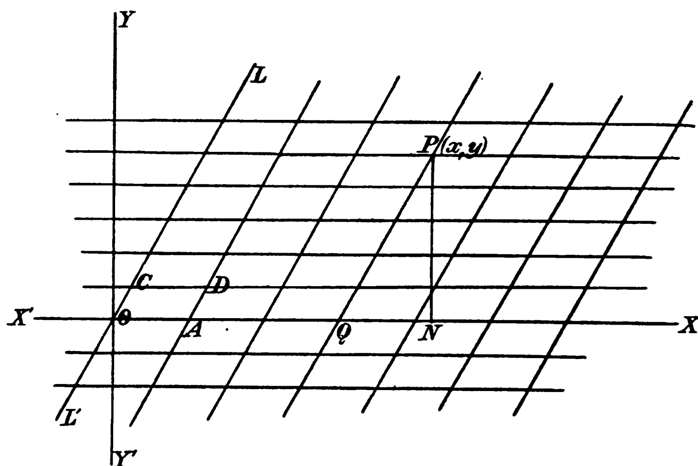


Fig. 3.

durch die Endpunkte der aufgetragenen Strecken Parallelen je zu der anderen Geraden. So wird die ganze Ebene in kongruente Parallelogramme zerlegt, deren jedes die Seiten $\sqrt{a}$, $\sqrt{c}$ und zwischen ihnen den Winkel φ, also den Inhalt

$$\sqrt{a} \cdot \sqrt{c} \cdot \sin\varphi = \frac{1}{2}\sqrt{4ac - b^2} = \sqrt{\frac{-D}{4}} \tag{34}$$

hat, während die Gitterpunkte, d. h. die Punkte, in denen die zwei Systeme von Parallelen sich durchkreuzen, diejenigen Punkte der Ebene sind, deren mit Bezug auf die Achsen $X'OX$, $L'OL$ genommenen Koordinaten

$$x \cdot \sqrt{a}, \quad y \cdot \sqrt{c}$$

sind, wenn x, y ganzzahlig gedacht werden. Somit ist das Quadrat der Entfernung eines jeden Gitterpunktes vom

Anfangspunkte zufolge einer bekannten trigonometrischen Formel gleich

$$(x\sqrt{a})^2 + 2 \cdot x\sqrt{a} \cdot y\sqrt{c} \cdot \cos\varphi + (y\sqrt{c})^2$$
$$= ax^2 + bxy + cy^2,$$

d. h. gleich dem Werte der quadratischen Form (a, b, c) für diejenigen ganzzahligen Werte der Unbestimmten x, y, welche den Gitterpunkt charakterisieren. Der Gesamtheit der Gitterpunkte entspricht daher die Gesamtheit der durch ganzzahlige x, y aus der Form entstehenden Werte oder die Gesamtheit der durch sie darstellbaren Zahlen, so zwar, daß jedem Gitterpunkte eine bestimmte dieser Zahlen zugeordnet ist, dieselbe Zahl m aber mehreren Gitterpunkten entsprechen kann, nämlich genau so vielen, als es verschiedene Darstellungen von m durch (a, b, c) gibt; es sind diejenigen, für welche das Quadrat des Abstandes von O

(35) $$ax^2 + bxy + cy^2 = m$$

ist, die also auf dem Kreise gelegen sind mit O als Mittelpunkt und $\sqrt{m}$ als Radius. Hiernach dürfen wir das konstruierte Gitter, welches wir, nur seine Gitterpunkte ins Auge fassend, wieder als Punktgitter bezeichnen, als geometrisches Bild der Form (a, b, c) betrachten, wenn deren Unbestimmte x, y ganzzahlig gedacht werden, oder können die Form durch das Punktgitter repräsentieren.

Ziehen wir nun die Gerade $Y'OY$ senkrecht zu $X'OX$ und nehmen diese beiden Geraden zu Koordinatenachsen, auf die wir jetzt die Lage jedes Gitterpunkts P beziehen. Aus der Figur entnimmt man für diese rechtwinkligen Koordinaten die Werte

$$X = OQ + QN = OQ + QP \cdot \cos\varphi = x\sqrt{a} + \frac{b}{2\sqrt{ac}} \cdot y\sqrt{c}$$

$$Y = PN = QP \cdot \sin\varphi = \frac{\sqrt{4ac - b^2}}{2\sqrt{ac}} \cdot y\sqrt{c}$$

oder

(36) $$X = \sqrt{a} \cdot x + \frac{b}{2\sqrt{a}} \cdot y, \qquad Y = \frac{\sqrt{-D}}{2\sqrt{a}} \cdot y,$$

Formeln, aus denen für die Grundpunkte A, C des Gitters die Koordinaten $\sqrt{a}$, 0 resp. $\frac{b}{2\sqrt{a}}, \frac{\sqrt{-D}}{2\sqrt{a}}$ hervorgehen, und für das Quadrat der Entfernung OP sich in der Tat wieder der Wert

$$(37)\qquad \begin{cases} X^2 + Y^2 = \left(\sqrt{a}\cdot x + \frac{b}{2\sqrt{a}}\cdot y\right)^2 - \frac{D}{4a}\cdot y^2 \\ \qquad\qquad = a x^2 + b x y + c y^2 \end{cases}$$

ergibt. Wenn nun, wie üblich, unter i die Quadratwurzel aus -1 verstanden, also $i^2 = -1$ gesetzt wird, so daß

$$X^2 + Y^2 = (X - iY)(X + iY)$$

geschrieben werden kann, so lehrt die letzterhaltene Beziehung eine Zerlegung der quadratischen Form $ax^2 + bxy + cy^2$ in zwei komplexe Linearfaktoren:

$$(38)\qquad a x^2 + b x y + c y^2 = \xi \cdot \xi',$$

wo

$$(39)\qquad \begin{cases} \xi = X + iY = \sqrt{a}\cdot x + \frac{b - \sqrt{D}}{2\sqrt{a}}\cdot y, \\ \xi' = X - iY = \sqrt{a}\cdot x + \frac{b + \sqrt{D}}{2\sqrt{a}}\cdot y \end{cases}$$

gedacht ist, eine Zerlegung, die auch unmittelbar aus der ersten der Formeln (11) zu entnehmen war. Diese Werte ξ, ξ' können ebensogut wie die ganzen Zahlen x, y zur Charakterisierung des Gitterpunkts benutzt werden und sollen deshalb zwei zueinander konjugierte Gitterzahlen genannt werden; werden sie gegeben:

$$\xi = X + iY, \quad \xi' = X - iY,$$

so liefern in der Tat ihre reellen Elemente X, Y die rechtwinkligen Koordinaten des Gitterpunktes, und so ist dieser Punkt in der von *Gauß* angegebenen Darstellungsweise komplexer Größen auch der geometrische Repräsentant der

komplexen Gitterzahl ξ, die ihrerseits als der zum Gitterpunkt gehörige Vektor bezeichnet werden kann*).

Die quadratische Form $ax^2 + bxy + cy^2$ aber kann als der algebraische Ausdruck für die Gesamtheit der Gitterzahlen aufgefaßt werden, welche dem Punktgitter entsprechen.

8. Gehen wir nunmehr zu Formen mit positiver Diskriminante über, so tritt uns auch hier eine Zerlegung der Form $ax^2 + bxy + cy^2$ in zwei Linearfaktoren entgegen, die aber jetzt reell sind**). In der Tat läßt sich aus der ersten der Formeln (11) die Gleichung

$$(40) \qquad ax^2 + bxy + cy^2 = \xi \cdot \xi'$$

entnehmen, wo wieder

$$(41) \quad \xi = \sqrt{a}\cdot x + \frac{b-\sqrt{D}}{2\sqrt{a}}\cdot y\,, \qquad \xi' = \sqrt{a}\cdot x + \frac{b+\sqrt{D}}{2\sqrt{a}}\cdot y$$

gefunden wird. Wir setzen jetzt

$$(42) \qquad X = \sqrt{a}\cdot x + \frac{b}{2\sqrt{a}}\cdot y\,, \qquad Y = \frac{\sqrt{D}}{2\sqrt{a}}\cdot y\,,$$

so daß

$$(43) \qquad \xi = X - Y\,, \qquad \xi' = X + Y$$

und

$$(44) \quad X^2 - Y^2 = (X-Y)(X+Y) = ax^2 + bxy + cy^2$$

---

*) Nach *Gauß* bedeutet die komplexe Größe $a + bi$ geometrisch den Punkt einer Ebene, welcher die rechtwinkligen Koordinaten a, b hat, oder, wenn $i = \sqrt{-1}$ als eine der Einheit gleiche Strecke aufgefaßt wird, welche gegen die Achse der reellen Größen senkrecht gerichtet ist, die Summe der beiden Vektoren $\bar{a}$ und $\overline{bi}$, d. h. den Vektor, welcher den Anfangspunkt mit dem Punkte a, b verbindet. Setzt man, ϱ positiv denkend,

$$a + bi = \varrho(\cos\psi + i\sin\psi)\,,$$

so ist ϱ die Länge und ψ die Richtung des letzteren, nämlich der Winkel, welchen dieser Vektor mit der Achse der reellen Größen einschließt.

**) Wir setzen dabei $a > 0$ voraus, was für unsere Zwecke keine Beschränkung ausmacht, da diese gestatten, eventuell die Form (a, b, c) durch eine andere ihr äquivalente mit positivem ersten Koeffizienten zu ersetzen; noch einfacher ist es, falls $a < 0$, im Texte unter $\sqrt{a}$ die Quadratwurzel aus dem Absolutwert von a zu verstehen.

wird, und fassen wieder X, Y als rechtwinklige Koordinaten eines Punktes auf. Auch hier können wir dann der Form ein genau wie vorher gebildetes Gitter entsprechen lassen. Den Werten $x=1$, $y=0$ entspricht nach den Formeln (42) der Punkt A (Fig. 3) mit den Koordinaten $X=\sqrt{a}$, $Y=0$ auf der Achse $X'OX$, den Werten $x=0$, $y=1$ der Punkt C mit den Koordinaten $X=\frac{b}{2\sqrt{a}}$, $Y=\frac{\sqrt{D}}{2\sqrt{a}}$; zieht man nun die Gerade $L'OCL$ und wiederholt mit den Strecken OA, OC auf den beiden Geraden $X'OX$, $L'OL$ die gleiche Konstruktion, wie vorher mit den Strecken $\sqrt{a}$, $\sqrt{c}$, so entsteht wieder ein aus lauter kongruenten Parallelogrammen bestehendes Gitter, dessen elementares Parallelogramm als Produkt aus Grundlinie und Höhe den Inhalt $\sqrt{a}\cdot\frac{\sqrt{D}}{2\sqrt{a}}=\sqrt{\frac{D}{4}}$ hat und für welches die rechtwinkligen Koordinaten aller Gitterpunkte, wie man leicht erkennt, durch die Größen (42) ausgedrückt werden, wenn darin für x, y alle ganzzahligen Werte gesetzt werden. Die Gitterpunkte können, wie durch diese Koordinaten, so auch wieder durch die Werte ξ, ξ' charakterisiert werden, denen daher auch hier der Name Gitterzahlen beigelegt werden soll, deren geometrische Bedeutung aber zwar einfach, doch von der vorigen abweichend ist. Denkt man sich nämlich die Geraden, welche die Winkel der Koordinatenachsen halbieren, so lauten deren Gleichungen in laufenden Koordinaten U, V bekanntlich

$$U-V=0\,,\qquad U+V=0\,,$$

und der Abstand eines Punkts mit den bestimmten Koordinaten X, Y von ihnen beträgt resp. $\frac{X-Y}{\sqrt{2}}$, $\frac{X+Y}{\sqrt{2}}$; somit bezeichnen die Gitterzahlen ξ, ξ' nichts anderes als die mit $\sqrt{2}$ multiplizierten Abstände des zugehörigen Gitterpunktes von jenen Halbierungslinien. Mit diesen Modifikationen hat man auch für positive Diskriminanten die quadratische Form als algebraischen Ausdruck für die Gesamtheit der Gitterzahlen zu betrachten, welche dem konstruierten Punktgitter entsprechen, das seinerseits das geometrische Bild der Form genannt werden darf.

Da jetzt der Gleichung $ax^2 + bxy + cy^2 = m$ die Gleichung

$$X^2 - Y^2 = m$$

entspricht, so liegen alle Gitterpunkte, welche den sämtlichen Darstellungen der Zahl m durch die quadratische Form zugehören, auf einer gleichseitigen Hyperbel mit O als Mittelpunkt und den Koordinatenachsen als Asymptoten. Hier müssen wir einer besonderen geometrischen Vorstellungsweise Erwähnung tun. Gewöhnlich versteht man unter dem Abstande eines Punktes der Ebene vom Anfangspunkte O den Radius des um O beschriebenen Kreises, auf welchem der Punkt liegt, oder betrachtet die um O beschriebenen Kreise

(45) $$X^2 + Y^2 = r^2$$

als Linien gleichen Abstandes von O. Läßt man nun jedem solchen Kreise die gleichseitige Hyperbel

(46) $$X^2 - Y^2 = r^2$$

entsprechen, so kann man die ganze Ebene ebensogut durch die Gesamtheit der Kreise wie durch die der Hyperbeln erfüllt denken oder sie im zweiten Falle als eine Abbildung der ursprünglichen Ebene auffassen, bei welcher jede Hyperbel das Bild der zugeordneten Kreislinie ist; man kann gewissermaßen die ursprüngliche Ebene so in sich umgeändert oder verzerrt, ihre Maßverhältnisse verwandelt denken, daß jeder Kreis in die ihm zugeordnete Hyperbel übergeht und demnach nun die Hyperbeln an die Stelle der Linien gleichen Abstandes von O treten oder als solche aufgefaßt werden dürfen. Diese in der neueren Geometrie vielfach übliche geometrische Maßvorstellung wollen wir als eine solche bezeichnen, bei welcher die Teile der Ebene nach hyperbolischem Maße gemessen werden.

Während wir nun im Falle einer negativen Diskriminante das Punktgitter, welches die quadratische Form repräsentiert, in gewöhnlicher Maßbestimmung auffassen, wollen wir dies im Falle einer positiven Diskriminante in hyperbolischer Maßbestimmung tun. Dann erhellt aus der Gleichung (44), daß auch in diesem Falle die quadratische Form $ax^2 + bxy + cy^2$ das Quadrat des (hyperbolischen) Abstandes eines Gitterpunktes vom Koordinatenanfange bezeichnet.

9. Dies vorausgeschickt, betrachten wir nun eine zweite Form

(47) $$f'(x', y') = a' x'^2 + b' x' y' + c' y'^2$$

mit der Diskriminante D', in welche die Form

(48) $$f(x, y) = a x^2 + b x y + c y^2$$

durch eine ganzzahlige Transformation

(49) $$x = \alpha x' + \beta y', \qquad y = \gamma x' + \delta y'$$

verwandelt wird, so daß nachstehende Gleichungen

(50) $$\begin{cases} a' = a \alpha^2 + b \alpha \gamma + c \gamma^2 \\ b' = (2 a \alpha + b \gamma) \beta + (b \alpha + 2 c \gamma) \delta \\ c' = a \beta^2 + b \beta \delta + c \delta^2 \end{cases}$$

statthaben.

Infolge der Transformationsgleichungen (49) besteht die Beziehung

(51) $$a x^2 + b x y + c y^2 = a' x'^2 + b' x' y' + c' y'^2$$

auch dann, wenn x, y bzw. x', y' ganz beliebige Werte bedeuten. Nun verschwindet die linke Seite dieser Gleichung, wenn für das Verhältnis $\frac{x}{y}$ eine Wurzel ω der Gleichung

(52) $$a z^2 + b z + c = 0,$$

d. i. einer der beiden Werte

(53) $$\omega_1 = \frac{-b + \sqrt{D}}{2 a}, \qquad \omega_2 = \frac{-b - \sqrt{D}}{2 a}$$

gesetzt wird; ebenso die rechte Seite, wenn für $\frac{x'}{y'}$ eine Wurzel der Gleichung

(54) $$a' z'^2 + b' z' + c' = 0,$$

d. i. einer der zwei Werte

(55) $$\omega_1' = \frac{-b' + \sqrt{D'}}{2 a'}, \qquad \omega_2' = \frac{-b' - \sqrt{D'}}{2 a'}$$

gesetzt wird. Da aber einem Werte von $\frac{x'}{y'}$, welcher die rechte Seite der Gleichung (51) zu Null macht, notwendig

ein solcher von $\frac{x}{y}$ entspricht, für welchen die linke Seite verschwindet, und da zwischen diesen Verhältnissen wegen (49) die Gleichung

$$\frac{x}{y} = \frac{\alpha x' + \beta y'}{\gamma x' + \delta y'} = \frac{\alpha \cdot \frac{x'}{y'} + \beta}{\gamma \cdot \frac{x'}{y'} + \delta}$$

besteht, so muß auch die folgende stattfinden:

$$\omega = \frac{\alpha \omega' + \beta}{\gamma \omega' + \delta}, \tag{56}$$

wenn unter ω ein beliebiger der Werte (53), unter ω' aber ein passender der Werte (55) verstanden wird. Man sieht leicht ein, daß sich hierbei die Wurzeln mit gleichem oder diejenigen mit entgegengesetztem Vorzeichen der Quadratwurzel entsprechen, je nachdem $\alpha\delta - \beta\gamma$ positiv oder negativ ist. Aus (56) folgt nämlich

$$\omega' = \frac{-\delta \omega + \beta}{\gamma \omega - \alpha}; \tag{57}$$

setzt man nun hierin $\omega = \frac{-b + \varepsilon\sqrt{D}}{2a}$, wo $\varepsilon = \pm 1$ gedacht ist, so folgt

$$\omega' = \frac{\delta b + 2a\beta - \varepsilon\delta\sqrt{D}}{-\gamma b - 2a\alpha + \varepsilon\gamma\sqrt{D}}$$

oder, wenn Zähler und Nenner mit $-\gamma b - 2a\alpha - \varepsilon\gamma\sqrt{D}$ multipliziert wird,

$$\omega' = \frac{-2a\left[(2a\alpha + b\gamma)\beta + (b\alpha + 2c\gamma)\delta - (\alpha\delta - \beta\gamma)\varepsilon\sqrt{D}\right]}{(2a\alpha + b\gamma)^2 - D\gamma^2}$$
$$= \frac{-\left[(2a\alpha + b\gamma)\beta + (b\alpha + 2c\gamma)\delta - (\alpha\delta - \beta\gamma)\varepsilon\sqrt{D}\right]}{2(a\alpha^2 + b\alpha\gamma + c\gamma^2)},$$

d. i. mit Rücksicht auf (50) und (25)

$$\omega' = \frac{-b' + (\alpha\delta - \beta\gamma)\varepsilon\sqrt{D}}{2a'} = \frac{-b' \pm \varepsilon\sqrt{D'}}{2a'}, \tag{58}$$

je nachdem $\alpha\delta - \beta\gamma$ positiv oder negativ ist.

Denkt man sich hiernach in der Gleichung (51) die quadratischen Formen in die beiden Faktoren zerlegt, die wir als ihre Gitterzahlen bezeichnet haben, indem man schreibt:

$$\left(\sqrt{a}\cdot x + \frac{b-\sqrt{D}}{2\sqrt{a}}\cdot y\right)\left(\sqrt{a}\cdot x + \frac{b+\sqrt{D}}{2\sqrt{a}}\cdot y\right)$$
$$= \left(\sqrt{a'}\cdot x' + \frac{b'-\sqrt{D'}}{2\sqrt{a'}}\cdot y'\right)\left(\sqrt{a'}\cdot x' + \frac{b'+\sqrt{D'}}{2\sqrt{a'}}\cdot y'\right),$$

so muß, wenn $\alpha\delta - \beta\gamma > 0$ ist,

$$\sqrt{a'}\cdot x' + \frac{b'-\sqrt{D'}}{2\sqrt{a'}}\cdot y' = \varrho\cdot\left(\sqrt{a}\cdot x + \frac{b-\sqrt{D}}{2\sqrt{a}}\cdot y\right)$$
$$\sqrt{a'}\cdot x' + \frac{b'+\sqrt{D'}}{2\sqrt{a'}}\cdot y' = \varrho^{-1}\cdot\left(\sqrt{a}\cdot x + \frac{b+\sqrt{D}}{2\sqrt{a}}\cdot y\right),$$

wenn aber $\alpha\delta - \beta\gamma < 0$ ist,

$$\sqrt{a'}\cdot x' + \frac{b'-\sqrt{D'}}{2\sqrt{a'}}\cdot y' = \varrho\cdot\left(\sqrt{a}\cdot x + \frac{b+\sqrt{D}}{2\sqrt{a}}\cdot y\right)$$
$$\sqrt{a'}\cdot x' + \frac{b'+\sqrt{D'}}{2\sqrt{a'}}\cdot y' = \varrho^{-1}\cdot\left(\sqrt{a}\cdot x + \frac{b-\sqrt{D}}{2\sqrt{a}}\cdot y\right)$$

sein, wo ϱ ein Proportionalitätsfaktor ist; je nach diesen beiden Fällen gehen also, vom letzteren abgesehen, die Faktoren der einen Form in die gleichnamigen resp. in die ungleichnamigen Faktoren der anderen Form über.

10. Bei der geometrischen Deutung dieser Resultate dürfen wir von dem Proportionalitätsfaktor absehen, da er nur den Maßstab der Figuren beeinflußt, ohne deren Ähnlichkeit aufzuheben. Dann entspricht also, je nachdem $\alpha\delta - \beta\gamma > 0$ oder < 0 ist, die Gitterzahl

$$\sqrt{a'}\cdot x' + \frac{b'-\sqrt{D'}}{2\sqrt{a'}}\cdot y'$$

der Form f' dem ersten oder zweiten der folgenden Ausdrücke:

$$(59\text{a})\quad\begin{cases}\sqrt{a}\cdot x+\dfrac{b-\sqrt{D}}{2\sqrt{a}}\cdot y=\left(\sqrt{a}\cdot\alpha+\dfrac{b}{2\sqrt{a}}\cdot\gamma\right)x'\\ \qquad+\left(\sqrt{a}\cdot\beta+\dfrac{b}{2\sqrt{a}}\cdot\delta\right)y'-\dfrac{\sqrt{D}}{2\sqrt{a}}(\gamma x'+\delta y'),\end{cases}$$

$$(59\text{b})\quad\begin{cases}\sqrt{a}\cdot x+\dfrac{b+\sqrt{D}}{2\sqrt{a}}\cdot y=\left(\sqrt{a}\cdot\alpha+\dfrac{b}{2\sqrt{a}}\cdot\gamma\right)x'\\ \qquad+\left(\sqrt{a}\cdot\beta+\dfrac{b}{2\sqrt{a}}\cdot\delta\right)y'+\dfrac{\sqrt{D}}{2\sqrt{a}}(\gamma x'+\delta y').\end{cases}$$

Man denke sich nun die Punkte A', C' mit den auf die Achsen OX, OY bezogenen rechtwinkligen Koordinaten

$$A'\colon \sqrt{a}\cdot\alpha+\frac{b}{2\sqrt{a}}\cdot\gamma,\quad \frac{\sqrt{\pm D}}{2\sqrt{a}}\cdot\gamma,$$

$$C'\colon \sqrt{a}\cdot\beta+\frac{b}{2\sqrt{a}}\cdot\delta,\quad \frac{\sqrt{\pm D}}{2\sqrt{a}}\cdot\delta,$$

wo das obere oder untere Vorzeichen gilt, je nachdem $D>0$ oder <0 ist, und die Punkte A'', C'' mit den Koordinaten:

$$A''\colon \sqrt{a}\cdot\alpha+\frac{b}{2\sqrt{a}}\cdot\gamma,\quad -\frac{\sqrt{\pm D}}{2\sqrt{a}}\cdot\gamma,$$

$$C''\colon \sqrt{a}\cdot\beta+\frac{b}{2\sqrt{a}}\cdot\delta,\quad -\frac{\sqrt{\pm D}}{2\sqrt{a}}\cdot\delta,$$

welche letzteren Punkte die Spiegelbilder der ersteren gegen die Achse OX sind. Verbindet man O mit A' und mit C' und bildet aus OA' und OC' in gleicher Weise wie früher aus OA und OC ein Gitter, so werden offenbar die rechtwinkligen Koordinaten seiner Gitterpunkte die folgenden sein:

$$(60\text{a})\quad\begin{cases}\left(\sqrt{a}\cdot\alpha+\dfrac{b}{2\sqrt{a}}\cdot\gamma\right)x'+\left(\sqrt{a}\cdot\beta+\dfrac{b}{2\sqrt{a}}\cdot\delta\right)y',\\ \dfrac{\sqrt{\pm D}}{2\sqrt{a}}(\gamma x'+\delta y').\end{cases}$$

Werden ebenso A'', C'' als Grundpunkte eines Gitters angesehen, so werden die Koordinaten seiner Gitterpunkte diese sein:

$$(60\text{b})\begin{cases}\left(\sqrt{a}\cdot\alpha+\frac{b}{2\sqrt{a}}\cdot\gamma\right)x'+\left(\sqrt{a}\cdot\beta+\frac{b}{2\sqrt{a}}\cdot\delta\right)y',\\ -\frac{\sqrt{\pm D}}{2\sqrt{a}}(\gamma x'+\delta y').\end{cases}$$

Nach der ersten der Formeln (50) ist aber $\sqrt{a'}$ die — je nachdem $D<0$ oder >0 ist, in gewöhnlicher oder hyperbolischer Maßbestimmung gedachte — Entfernung OA' oder OA''. Man ersieht hieraus, daß, entsprechend den beiden Fällen (59a), (59b), d. h. je nachdem $\alpha\delta-\beta\gamma>0$ oder <0 ist, das erste resp. zweite der soeben gebildeten Gitter dasjenige der Form f' ist, wenn dies von der Achse OA' bzw. OA'' aus ebenso konstruiert wird, wie das Gitter der Form f von der Achse OA aus konstruiert worden ist. In der Tat: die Gitterzahlen seiner Grundpunkte entsprechen den Annahmen $x'=1$, $y'=0$ resp. $x'=0$, $y'=1$, demnach fallen nach (60a) bzw. (60b) die Grundpunkte mit A', C' bzw. mit A'', C'' zusammen. Nun sind die Grundpunkte A', C' des ersten jener Gitter und demnach auch seine sämtlichen Gitterpunkte zugleich auch Gitterpunkte des zur Form f gehörigen Gitters oder, kürzer gesagt, das gesamte erstgenannte Gitter ist dem letzteren eingelagert, d. h. ein Teil desselben. Demnach ist zu schließen:

Geht die Form f durch eine Transformation (49), deren Determinante $\alpha\delta-\beta\gamma$ positiv ist, in die Form f' über, so läßt sich das Gitter der neuen Form demjenigen der ursprünglichen einlagern. Sein Elementarparallelogramm, welches den Inhalt $\sqrt{\frac{\pm D'}{4}}$ hat, ist das Parallelogramm mit den Seiten OA', OC', dessen durch die Koordinaten der Punkte A', C' ausgedrückter Inhalt in der Tat gleich dem Absolutwerte von

$$\left(\sqrt{a}\cdot\alpha+\frac{b}{2\sqrt{a}}\cdot\gamma\right)\cdot\frac{\sqrt{\pm D}}{2\sqrt{a}}\delta-\left(\sqrt{a}\cdot\beta+\frac{b}{2\sqrt{a}}\cdot\delta\right)\frac{\sqrt{\pm D}}{2\sqrt{a}}\gamma$$
$$=(\alpha\delta-\beta\gamma)\cdot\sqrt{\frac{\pm D}{4}},$$

d. i. der Formel (25) zufolge gleich $\sqrt{\frac{\pm D'}{4}}$ gefunden wird. Da dasjenige des zu f gehörigen Gitters gleich $\sqrt{\frac{\pm D}{4}}$ ist, so besteht zwischen den Inhalten I, I' beider Elementarparallelogramme die Beziehung

$$I' = (\alpha\delta - \beta\gamma) \cdot I,$$

und sie werden also dann und nur dann einander gleich sein, wenn $\alpha\delta - \beta\gamma = 1$, d. h. wenn die Formen f, f' einander (eigentlich) äquivalent sind.

Da aber in diesem Falle $f(x, y)$ aus $f'(x', y')$ durch eine ganzzahlige Transformation von ganz derselben Art entsteht, wie $f'(x', y')$ aus $f(x, y)$, so muß auch das Punktgitter der ersteren Form ein Teil desjenigen der zweiten sein, mithin beide Punktgitter sich decken, wobei der Punkt x', y' des neuen Gitters mit dem durch die Gleichungen (49) bestimmten Punkte x, y des ursprünglichen identisch ist.

Wenn die Determinante $\alpha\delta - \beta\gamma$ der Transformation (49), statt positiv zu sein, negativ ist, so ist das Gitter, welches zur neuen Form f' gehört, das Spiegelbild des eben besprochenen gegen die Achse OX.

Für den Fall äquivalenter Formen entnehmen wir diesen Auseinandersetzungen den **Satz:**

Zwei äquivalenten Formen entspricht als geometrisches Bild das nämliche Punktgitter. Bei eigentlicher Äquivalenz deckt sich das Gitter der einen beider Formen vollständig mit demjenigen der andern, nur daß es auf andere Weise in Elementarparallelogramme derselben Größe wie das des letzteren angeordnet erscheint. Somit darf dann dies Gitter als geometrisches Bild nicht nur der einzelnen Form $f(x, y)$, sondern auch als dasjenige der ganzen Klasse eigentlich äquivalenter Formen angesehen werden, welcher die Form $f(x, y)$ angehört. Bei uneigentlicher Äquivalenz der Formen ist dagegen das eine der Gitter das an OX gespiegelte Bild des vorigen, oder gleich diesem, aber so gesehen, wie es von der Rückseite der Ebene aus erscheint.

11. Ist z. B. f' die Form f mit entgegengesetztem mittleren Koeffizienten, zwei Formen, die wir nach *Gauß*

einander entgegengesetzt nennen, so geht f in f' über durch die Transformation

$$x = x', \quad y = -y',$$

die beiden Formen sind also einander uneigentlich äquivalent. Aus dem Gitter der ersten findet man das der andern, wenn man bedenkt, daß dessen Grundpunkte nach (36), (42) resp. die Koordinaten $\sqrt{a}$, 0; $\frac{-b}{2\sqrt{a}}$, $\frac{+\sqrt{\pm D}}{2\sqrt{a}}$ haben, also (s. Fig. 4) der Punkt A und der zu C gegen OX symmetrisch liegende Punkt C_1 sind; mithin ist $A\,O\,C_1\,D_1$ das Elementarparallelo-

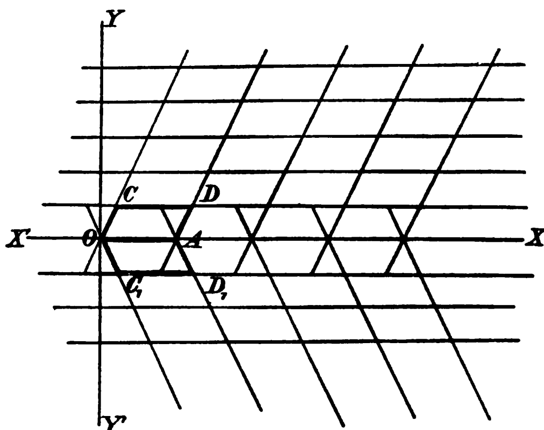


Fig. 4.

gramm des neuen Gitters, d. i. dasjenige des ursprünglichen, aber so gesehen, wie es von der Rückseite der Ebene aus erscheint.

Bedeutet nun allgemeiner $f'(x', y')$ irgend eine der Form

$$f(x, y) = a x^2 + b x y + c y^2$$

uneigentlich äquivalente Form und (49) die Transformation, durch welche sie aus $f(x, y)$ entsteht, so kann man die letztere durch die Folge zweier Transformationen:

$$x = \alpha x'' - \beta y'', \quad y = \gamma x'' - \delta y''$$
$$x'' = x', \quad y'' = -y'$$

hervorbringen, für deren erste die Determinante

$$\alpha(-\delta) - (-\beta)\gamma = +1,$$

für deren zweite sie -1 ist; nennt man $f''(x'', y'')$ die Form, in welche $f(x, y)$ durch die erste übergeht, so muß $f''(x'', y'')$ durch die zweite sich in $f'(x', y')$ verwandeln und somit der letzteren Form entgegengesetzt sein, andererseits ist sie mit $f(x, y)$ eigentlich äquivalent. Ist demnach $f(x, y)$ mit einer Form uneigentlich äquivalent, so ist sie es eigentlich mit der zur letztern entgegengesetzten Form, und offenbar auch umgekehrt. Da hiernach die Frage nach der uneigentlichen Äquivalenz zweier Formen auf die nach der eigentlichen Äquivalenz zweier anderen zurückkommt, dürfen und wollen wir fortan, wenn nicht ausdrücklich das Gegenteil gesagt wird, die Untersuchung auf eigentliche Äquivalenz beschränken.

12. Zum Schluß dieser Betrachtungen heben wir unter allen Formen mit der Diskriminante D eine besonders ausgezeichnete hervor. Sie hat verschiedene Gestalt, je nachdem die Diskriminante

$$D = d \equiv 1 \pmod{4}$$

oder

$$D = 4d \equiv 0 \pmod{4}$$

ist. Im ersten Falle ist $\frac{1-d}{4}$ eine ganze Zahl und die Form

$$x^2 + xy + \frac{1-d}{4} \cdot y^2 \tag{61}$$

eine solche mit der Diskriminante $1 - 4 \cdot \frac{1-d}{4} = d = D$. Andernfalls hat die Form

$$x^2 - dy^2 \tag{62}$$

die Diskriminante $4d = D$. Diese Formen sollen je die Hauptform mit der Diskriminante D, und die Klasse äquivalenter Formen, der sie angehört, die Hauptklasse heißen. Für das Gitter der ersteren haben die Grundpunkte die Koordinaten 1, 0 resp. $\frac{1}{2}$, $\frac{\sqrt{\pm d}}{2}$; da somit der Punkt C

senkrecht über die Mitte M von OA (Fig. 5) zu stehen kommt, so sind die Dreiecke OMC und AMC kongruent

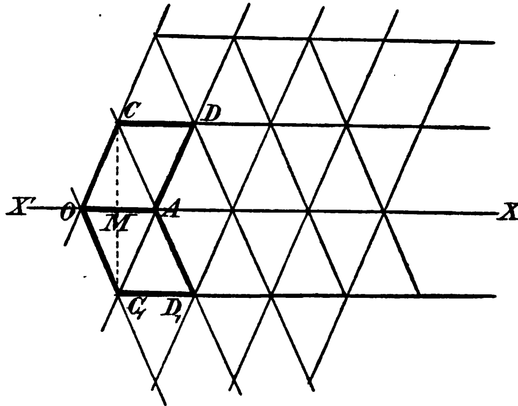


Fig. 5.

und das Parallelogramm $OCAC_1$, das an Inhalt dem Elementarparallelogramm $OCDA$ gleichkommt, ist ein Rhom-

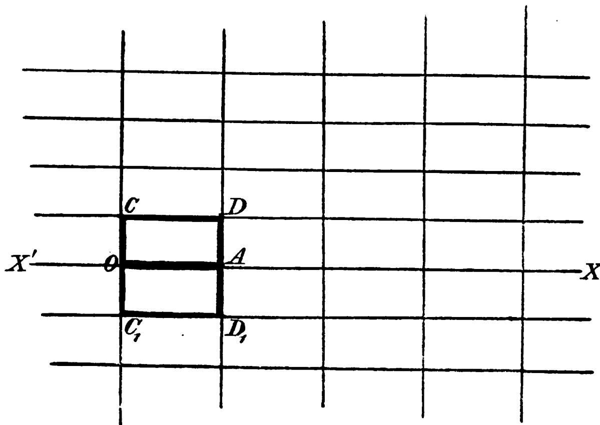


Fig. 6.

bus. Daher läßt sich das Gitter jetzt in lauter kongruente Rhomben zerlegen und ist dann mit dem von der Rückseite der Ebene gesehenen, ebenso zerlegten Gitter der entgegen-

gesetzten Form identisch. Das Gleiche ereignet sich offenbar allgemeiner stets dann, wenn in der quadratischen Form (a, b, c) der mittlere Koeffizient b dem ersten a gleich ist, denn dann haben die Grundpunkte A, C die Koordinaten $\sqrt{a}, 0;\ \frac{1}{2}\sqrt{a}, \frac{\sqrt{\pm D}}{2\sqrt{a}}$ resp. und C steht wieder über der Mitte von OA.

Im zweiten Falle haben die Grundpunkte für das Gitter der Hauptform (62) die Koordinaten 1, 0; $0, \sqrt{\pm d}$ resp., der Punkt C fällt mithin auf die Y-Achse und das Elementarparallelogramm wird ein Rechteck (Fig. 6). Das Gitter besteht also in diesem Falle aus lauter kongruenten Rechtecken, und so bietet das Gitter der entgegengesetzten Form, welche jetzt mit der ursprünglichen identisch ist, von der Rückseite der Ebene gesehen wieder den gleichen Anblick.

Was endlich die Gitterzahlen der Hauptform betrifft, so sind sie für die Hauptform (61) die folgenden:

$$(61\,\mathrm{a})\qquad \xi = x + \frac{1-\sqrt{d}}{2}\cdot y, \qquad \xi' = x + \frac{1+\sqrt{d}}{2}\cdot y,$$

für die Hauptform (62) dagegen diese:

$$(62\,\mathrm{a})\qquad \xi = x - y\sqrt{d}, \qquad \xi' = x + y\sqrt{d},$$

ein Ergebnis, auf dessen Bedeutung wir später zurückkommen werden.

13. Die in Nr. 10 angestellte Erwägung hat zu einem Gesichtspunkte geführt, das Problem der Äquivalenz zweier Formen wieder von einer neuen Seite zu betrachten. Aus der eigentlichen Äquivalenz der Formen (a, b, c) und (a', b', c') schlossen wir die Beziehung

$$(63)\qquad \omega = \frac{\alpha\omega' + \beta}{\gamma\omega' + \delta}$$

zwischen den gleichnamigen Wurzeln der Formen unter Geltung der Gleichung $\alpha\delta - \beta\gamma = 1$, d. h. nach früherer Ausdrucksweise die eigentliche Äquivalenz der Zahlen ω, ω'. Es läßt sich aber auch umgekehrt aus der letzteren die erstere Äquivalenz folgern, wenn die Formen als solche mit derselben Diskriminante gedacht werden. In der Tat, setzt

man, indem man $\sqrt{D}$ mit beliebigem, aber beidemal gleichem Vorzeichen genommen denkt, in (63)

$$\omega = \frac{-b+\sqrt{D}}{2a}, \quad \omega' = \frac{-b'+\sqrt{D}}{2a'} \tag{64}$$

ein, so nimmt die Formel die Gestalt

$$\frac{-b+\sqrt{D}}{2a} = \frac{2a'\beta - b'\alpha + \alpha\sqrt{D}}{2a'\delta - b'\gamma + \gamma\sqrt{D}}$$

an, die, wenn rechts mit $2a'\delta - b'\gamma - \gamma\sqrt{D}$ erweitert wird, nach einfacher Rechnung in die folgende:

$$\frac{-b+\sqrt{D}}{2a} = \frac{(2a'\beta - b'\alpha)\delta + (-b'\beta + 2c'\alpha)\gamma + \sqrt{D}}{2(a'\delta^2 - b'\gamma\delta + c'\gamma^2)} \tag{65}$$

übergeht. Aus dieser aber erschließt man durch Vergleichung des Rationalen bzw. des Irrationalen auf beiden Seiten

$$a = a'\delta^2 - b'\gamma\delta + c'\gamma^2 = f'(\delta, -\gamma), \tag{66a}$$

$$b = -(2a'\delta - b'\gamma)\beta + (b'\delta - 2c'\gamma)\alpha \tag{66b}$$

und mit Rücksicht auf die aus der Grundformel (9) hervorgehende Gleichung

$$\left\{\begin{aligned} & 4\cdot f'(\delta, -\gamma) f'(-\beta, \alpha) \\ & = [-(2a'\delta - b'\gamma)\beta + (b'\delta - 2c'\gamma)\alpha]^2 - D \end{aligned}\right. \tag{67}$$

die Gleichheit

$$4a\cdot f'(-\beta, \alpha) = b^2 - D = 4ac$$

also

$$c = f'(-\beta, \alpha) = a'\beta^2 - b'\beta\alpha + c'\alpha^2. \tag{66c}$$

Die so für a, b, c erhaltenen Ausdrücke zeigen, daß die Form (a, b, c) aus der Form (a', b', c') mittels der Transformation

$$x' = \delta x - \beta y, \quad y' = -\gamma x + \alpha y$$

hervorgeht, deren Koeffizienten die Bedingung erfüllen

$$\delta\cdot\alpha - (-\beta)(-\gamma) = 1,$$

d. h. daß beide Formen eigentlich äquivalent sind.

Die eigentliche Äquivalenz zweier Formen gleicher Diskriminante ist demnach identisch mit

der eigentlichen Äquivalenz ihrer gleichnamigen Wurzeln. Somit darf die Frage nach jener durch die Frage nach der letzteren ersetzt werden, und wir wollen in der Tat dementsprechend verfahren.

Indem wir für die Zahl D die Voraussetzungen festhalten, die ihr als einer Stammdiskriminante zukommen, betrachten wir die Gesamtheit Ω aller Zahlen von der Form

$$\frac{-b+\sqrt{D}}{2a},$$

worin a, b ganze Zahlen und $b^2 \equiv D \pmod{4a}$ ist. Sie ist zugleich die Gesamtheit der ersten Wurzeln aller (primitiven) quadratischen Formen mit der Diskriminante D; in der Tat gehören diese sämtlich ihr an, andererseits ist jede Zahl $\omega = \frac{-b+\sqrt{D}}{2a}$ der gedachten Art die Wurzel der Gleichung

$$(2a\omega + b)^2 = D,$$

welcher die Gestalt

$$4a^2\omega^2 + 4ab\omega + b^2 - D = 0$$

oder, da nach den Voraussetzungen, unter c eine ganze Zahl verstanden, $b^2 - D = 4ac$ gesetzt werden darf, die Gestalt

$$a\omega^2 + b\omega + c = 0$$

gegeben werden kann, während a, b, c (s. Ende von Nr. 3) ohne gemeinsamen Teiler sind, also ist ω die erste Wurzel der (primitiven) quadratischen Form (a, b, c) mit der Diskriminante D. Dem Gesagten zufolge wird also die Einteilung dieser Formen in Klassen äquivalenter Formen mit der Einteilung der Zahlen der Gesamtheit Ω in Klassen äquivalenter Zahlen vollständig sich decken.

14. Um diese nun zu leisten, muß man verschieden verfahren im Falle einer negativen und im Falle einer positiven Diskriminante.

Wir setzen zuerst $D < 0$ voraus. Da es sich in diesem Falle nur um positive Formen handelt, ist der Nenner der Zahl $\omega = \frac{-b+\sqrt{D}}{2a}$ positiv, die Zahl

$$\omega = \frac{-b}{2a} + i \cdot \frac{\sqrt{-D}}{2a}$$

selbst komplex mit dem reellen Bestandteile $\frac{-b}{2a}$. Nennt man nun b_1 den absolut kleinsten Rest von $-b$ (mod. $2a$) und setzt in dem Falle, wo $-b$ ein ungerades Vielfaches von a ist, als absolut kleinster Rest (mod. $2a$) also sowohl $+a$ wie $-a$ genommen werden kann, der Bestimmtheit wegen $b_1 = +a$, so gelten die Ungleichheiten

$$-a < b_1 \gtreqless a \qquad \text{oder} \qquad -\tfrac{1}{2} < \frac{b_1}{2a} \gtreqless \tfrac{1}{2},$$

so daß, wenn $-b = 2az + b_1$ gesetzt wird, z die am nächsten an $\frac{-b}{2a}$ liegende ganze Zahl bezeichnet. Man schließt weiter $b^2 \equiv b_1^2$ (mod. $4a$), also wird $\frac{b_1^2 - D}{4a}$ zugleich mit $\frac{b^2 - D}{4a}$ eine positive ganze Zahl sein, welche a_1 genannt werde. Nun setze man

(68) $$\bar{\omega} = \omega - z = \frac{b_1 + \sqrt{D}}{2a}$$

und

(69) $$\omega_1 = -\frac{1}{\bar{\omega}};$$

dann ergibt sich leicht $\omega_1 = \frac{-b_1 + \sqrt{D}}{2a_1}$, während, wenn ω' die konjugiert imaginäre Zahl zu ω bezeichnet,

(70) $$(\omega - z)(\omega' - z) = \frac{b_1^2 - D}{4a^2} = \frac{a_1}{a}$$

gefunden wird. In gleicher Weise kann man fortfahren; bezeichnet b_2 wieder den wie vorher bestimmten absolut kleinsten Rest von $-b_1$ (mod. $2a_1$), z_1 die zunächst an $\frac{-b_1}{2a_1}$ liegende ganze Zahl und a_2 die positive ganze Zahl $\frac{b_2^2 - D}{4a_1}$, so folgen aus

(71) $$\bar{\omega}_1 = \omega_1 - z_1 = \frac{b_2 + \sqrt{D}}{2a_1}$$

und

(72) $$\omega_2 = -\frac{1}{\bar{\omega}_1}$$

die Gleichungen

$$\omega_2 = \frac{-b_2 + \sqrt{D}}{2\,a_2} \qquad \text{und} \qquad (\omega_1 - z_1)(\omega_1' - z_1) = \frac{a_2}{a_1}$$

usw. Aber die positiven ganzen Zahlen $a, a_1, a_2, \ldots$ können nicht ohne Ende abnehmen, bei Fortsetzung des Verfahrens muß man also zu einer Zahl a_{i+1} kommen, welche gleich oder größer ist als die vorhergehende Zahl a_i. Aus der zur letzteren gehörigen Zahl ω_i erhält man dann durch die Gleichung

(73) $$\omega_0 = \omega_i - z_i = \frac{b_{i+1} + \sqrt{D}}{2\,a_i}$$

eine Zahl ω_0, für welche der reelle Bestandteil zwischen $-\frac{1}{2}$ exkl. und $+\frac{1}{2}$ inkl. enthalten,

$$\omega_0 \cdot \omega_0' = (\omega_i - z_i)(\omega_i' - z_i) = \frac{a_{i+1}}{a_i}$$

aber gleich oder größer als 1 ist, so daß, wenn

(74) $$\omega_0 = \xi + \eta\, i$$

gesetzt wird, die Ungleichheiten erfüllt sind

(75) $$-\tfrac{1}{2} < \xi \leqq \tfrac{1}{2}, \qquad \xi^2 + \eta^2 \geqq 1\,.$$

Wir wollen eine Zahl ω_0, welche diese Bedingungen erfüllt, eine **reduzierte Zahl** nennen.

Die auf solche Weise gewonnenen Zahlen

$$\omega,\ \overline{\omega},\ \omega_1,\ \overline{\omega}_1,\ \omega_2,\ \ldots,\ \omega_i,\ \omega_0$$

sind aber jede der vorhergehenden, sämtlich also der ersten eigentlich äquivalent, und zwar geht wegen $\omega = \overline{\omega} + z$ die erste aus $\overline{\omega}$ durch die Substitution S:

$$\omega = \frac{1 \cdot \overline{\omega} + z}{0 \cdot \overline{\omega} + 1},$$

$\overline{\omega}$ aber wegen $\overline{\omega} = -\dfrac{1}{\omega_1}$ aus ω_1 durch die Substitution T:

$$\overline{\omega} = \frac{0 \cdot \omega_1 - 1}{1 \cdot \omega_1 + 0},$$

nun wieder ω_1 aus $\overline{\omega}_1$ durch die Substitution S_1:

$$\omega_1 = \frac{1 \cdot \overline{\omega}_1 + z_1}{0 \cdot \overline{\omega}_1 + 1},$$

dann $\overline{\omega}_1$ aus ω_2 durch die Substitution T:

$$\overline{\omega}_1 = \frac{0 \cdot \omega_2 - 1}{1 \cdot \omega_2 + 0}$$

hervor, usw., so daß endlich ω aus ω_0 gewonnen wird durch eine zusammengesetzte Substitution, welche folgendermaßen geschrieben werden kann:

(76) $$ST \cdot S_1 T \ldots S_{i-1} T \cdot S_i .$$

Wir schließen also aus der angestellten Betrachtung den

Satz: Im Falle einer negativen Diskriminante ist jede Zahl ω der Gesamtheit Ω einer reduzierten Zahl ω_0 dieser Gesamtheit eigentlich äquivalent.

15. Übertragen wir dies zunächst von den Zahlen der Gesamtheit Ω auf die ihnen entsprechenden quadratischen Formen. Der Substitution ST, durch welche

$$\omega = \frac{z\,\omega_1 - 1}{1 \cdot \omega_1 + 0}$$

gesetzt wird, entspricht eine Transformation

(77) $$x = z x' - y', \qquad y = x',$$

durch welche die der Zahl ω entsprechende quadratische Form

(78) $$a x^2 + b x y + c y^2$$

in den Ausdruck

$$(a z^2 + b z + c) \cdot x'^2 - (2 a z + b) \cdot x' y' + a \cdot y'^2$$

übergeht, in welchem

$$-(2 a z + b) = b_1$$

und

$$a z^2 + b z + c = \frac{4 a^2 z^2 + 4 a b z + 4 a c}{4 a} = \frac{b_1^2 - D}{4 a} = a_1$$

ist; die Form (78) verwandelt sich also durch die Transformation (77) in eine eigentlich äquivalente Form

(79) $$a_1 x'^2 + b_1 x' y' + a y'^2,$$

welche die Besonderheit darbietet, daß ihr dritter Koeffizient dem ersten der Form (78) gleich, die Summe der beiden mittleren Koeffizienten aber durch das Doppelte $2a$ des

gemeinsamen Koeffizienten teilbar und der Quotient $\frac{b+b_1}{2a}$ dem Substitutionskoeffizienten z entgegengesetzt gleich ist. Um dieser Eigenschaft der neuen Form willen mag sie der Form (78) (nach links hin) benachbart heißen. Durch die Transformation

$$x' = z_1 x'' - y'', \quad y' = x'',$$

welche der Substitution $S_1 T$ entspricht, geht die neue Form in die ihr wieder (links) benachbarte Form

$$a_2 x''^2 + b_2 x'' y'' + a_1 y''^2$$

über usw.; durch eine der Transformation $S_{i-1} T$ entsprechende Transformation entsteht die der voraufgehenden Form nach links benachbarte Form $a_i x^2 + b_i x y + a_{i-1} y^2$, aus welcher endlich durch die Transformation

$$x = x' + z_i y', \quad y = y',$$

welche der Substitution S_i entspricht, die Form

$$a_i x'^2 + (2 a_i z_i + b_i) x' y' + (a_i z_i^2 + b_i z_i + a_{i-1}) y'^2,$$

d. i. die Form

(80) $$a_i x'^2 - b_{i+1} x' y' + a_{i+1} y'^2$$

hervorgeht, deren Koeffizienten den Bedingungen genügen:

(81) $$-a_i < b_{i+1} \lesseqgtr a_i \lesseqgtr a_{i+1}.$$

Wird eine solche Form eine reduzierte Form geheißen, so darf man dem zuvor erhaltenen Satze den entsprechenden substitutieren:

Jede Form mit negativer Diskriminante ist einer reduzierten Form eigentlich äquivalent. Die angestellte Betrachtung liefert zudem auch eine Methode, um eine Transformation anzugeben, welche jene in diese verwandelt.

16. Wir leiten aus dem Vorigen zunächst einen äußerst wichtigen Satz her.

Die Bedingungen (75), denen eine reduzierte Zahl

$$\omega_0 = \frac{-b + \sqrt{D}}{2a} = \xi + \eta i$$

unterworfen ist, ergeben $\xi^2 \leqq \frac{1}{4}$, mithin

$$\eta^2 \geqq 1 - \xi^2 \geqq \tfrac{3}{4} \tag{82}$$

oder, da $\eta = \frac{\sqrt{-D}}{2a}$ ist,

$$a \leqq \sqrt{\frac{-D}{3}}, \tag{83}$$

während $-a < b \leqq a$, b also numerisch ebenfalls kleiner als $\sqrt{\frac{-D}{3}}$ ist; da hiernach die ganzen Zahlen a, b nur eine endliche Anzahl von Werten annehmen können, ist auch die Anzahl der reduzierten Zahlen ω_0 nur endlich. Weil aber jede Zahl in Ω einer reduzierten Zahl äquivalent ist, dürfen diese zu Repräsentanten der sämtlichen Klassen äquivalenter Zahlen gewählt werden, und somit kann die Anzahl der letzteren gewiß nicht größer sein als die der reduzierten Zahlen; man hat daher den

Satz: Die Anzahl Klassen eigentlich äquivalenter Zahlen der Gesamtheit Ω oder der ihnen entsprechenden quadratischen Formen mit der negativen Diskriminante D ist endlich.

Es fragt sich nur, ob sie nicht noch kleiner ist als die der reduzierten Zahlen, indem etwa von diesen selbst mehrere untereinander äquivalent werden. Um dies zu entscheiden, seien

$$\omega_0 = \frac{-b + \sqrt{D}}{2a}, \qquad \omega_0^{(1)} = \frac{-b' + \sqrt{D}}{2a'}$$

zwei verschiedene reduzierte Zahlen, also

$$-a < b \leqq a \leqq c = \frac{b^2 - D}{4a}$$

$$-a' < b' \leqq a' \leqq c' = \frac{b'^2 - D}{4a'}.$$

Setzen wir, was erlaubt ist, $a' \geqq a$ voraus und nehmen dann an, ω_0 und $\omega_0^{(1)}$ seien eigentlich äquivalent, also

$$\omega_0 = \frac{\alpha\,\omega_0^{(1)} + \beta}{\gamma\,\omega_0^{(1)} + \delta},$$

während $\alpha\delta - \beta\gamma = 1$. Nach Nr. 13 ergeben sich dann die Beziehungen

$$(84)\qquad \begin{cases} a = a'\delta^2 - b'\gamma\delta + c'\gamma^2 \\ b = -(2a'\delta - b'\gamma)\beta + (b'\delta - 2c'\gamma)\alpha\,, \end{cases}$$

deren erstere auch in der Gestalt

$$(85)\qquad 4aa' = (2a'\delta - b'\gamma)^2 - D\gamma^2$$

geschrieben werden kann. Da nun für die reduzierten Zahlen ω_0, $\omega_0^{(1)}$ nach (83)

$$a \lesseqgtr \sqrt{\frac{-D}{3}} \quad \text{und ebenso} \quad a' \lesseqgtr \sqrt{\frac{-D}{3}}$$

ist, so ist $4aa' \lesseqgtr \frac{-4D}{3}$, während der Ausdruck zur Rechten der vorigen Gleichung, wenn $\gamma^2 > 1$ wäre, mindestens gleich $-4D$ wäre. Somit muß entweder $\gamma = 0$ oder $\gamma = \pm 1$ sein.

Ist $\gamma = 0$, also $\alpha\delta = 1$, so folgt aus (85) die Gleichheit $a = a'$ und aus der zweiten der Gleichungen (84) $b - b' = \mp 2a'\beta$, also teilbar durch $2a'$. Da aber b, b' numerisch nicht größer als a resp. a', beide also nicht größer als a' sind, so kann $b - b'$ numerisch höchstens gleich $2a'$ sein; man schließt daher, daß entweder $b - b' = 0$, also gegen die Voraussetzung $\omega_0 = \omega_0^{(1)}$ wäre, oder $b - b' = \pm 2a'$, mithin eine der Zahlen b, b' gleich $+a' = a$, die andere gleich dem ausgeschlossenen Werte $-a' = -a$; diese Voraussetzung ist also unzulässig.

Ist dagegen $\gamma = \pm 1$, so folgt aus der ersten der Gleichungen (84)

$$(86)\qquad a = a'\delta^2 \mp b'\delta + c'\,;$$

da aber $a \lesseqgtr a' \lesseqgtr c'$, muß $a'\delta^2 \mp b'\delta \lesseqgtr 0$ sein, während doch andererseits, da b' numerisch nicht größer als a' ist, $b'\delta$ numerisch nicht größer als $a'\delta^2$ sein kann, also $a'\delta^2 \mp b'\delta \geqq 0$ sein muß. So findet sich

$$(87)\qquad a'\delta^2 \mp b'\delta = 0.$$

Demnach geht aus (86) $a = c'$ hervor, was in Verbindung mit $a \lesseqgtr a' \lesseqgtr c'$ die Gleichheit $a = a' = c'$ ergibt. Nunmehr läßt sich mit Rücksicht auf (86) und auf die Glei-

chung $\alpha\delta - \beta\gamma = 1$ der zweiten der Formeln (84) die Gestalt

$$b + b' = 2a'(-\beta\delta \pm \alpha\delta^2 \mp \alpha)$$

geben, $b + b'$ wäre also teilbar durch $2a'$, was, da b, b' numerisch nicht größer als $a = a'$ sind, nur sein kann, wenn entweder $b + b' = \pm 2a'$, also $b = b' = a = a'$, mithin gegen die Voraussetzung $\omega_0 = \omega_0^{(1)}$ wäre, oder wenn $b = -b'$ ist, woraus mit Rücksicht auf die Gleichungen

$$a = a' = c', \qquad b'^2 - 4a'c' = b^2 - 4ac$$

auch $a = c$ hervorgeht. Dann würde aber

$$\omega_0 = \frac{b' + \sqrt{D}}{2a'} = -\frac{1}{\omega_0^{(1)}}$$

sein. In diesem einzigen Falle können also die beiden reduzierten Zahlen ω_0, $\omega_0^{(1)}$ oder die beiden ihnen entsprechenden reduzierten Formen

$$(a, b, a), \qquad (a, -b, a)$$

einander (eigentlich) äquivalent sein und sind es in der Tat, da ω_0 aus $\omega_0^{(1)}$ durch die Substitution

$$\omega_0 = \frac{0 \cdot \omega_0^{(1)} - 1}{1 \cdot \omega_0^{(1)} + 0}$$

hervorgeht.

Durch diese Resultate sind wir nun in den Stand gesetzt, für zwei quadratische Formen mit negativer Diskriminante die Frage nach ihrer Äquivalenz zu lösen. Man suche in der in Nr. 15 angegebenen Weise die reduzierten Formen auf, denen sie äquivalent sind; wenn diese identisch miteinander oder zwei reduzierte Formen der erwähnten besonderen Art sind, so werden auch die fraglichen Formen äquivalent sein, und man kann eine Transformation der einen in die andere angeben; entgegengesetztenfalls sind sie nicht äquivalent.

17. Auch die Reduktion der quadratischen Formen läßt geometrische Deutungen zu. Denkt man sich in der oben nach *Gauß* angemerkten Weise die Zahl

$$\omega = \frac{-b + \sqrt{D}}{2a} = \xi + \eta i$$

als Punkt einer Ebene mit den rechtwinkligen Koordinaten ξ, η abgebildet, so liegt jeder Punkt der Gesamtheit Ω in der positiven Halbebene, da $\eta = \frac{\sqrt{-D}}{2a}$ positiv ist. Den komplexen Werten $\xi + \eta i$, für welche $-\frac{1}{2} < \xi$ ist, entsprechen Punkte zur Rechten der Geraden QN (Fig. 7),

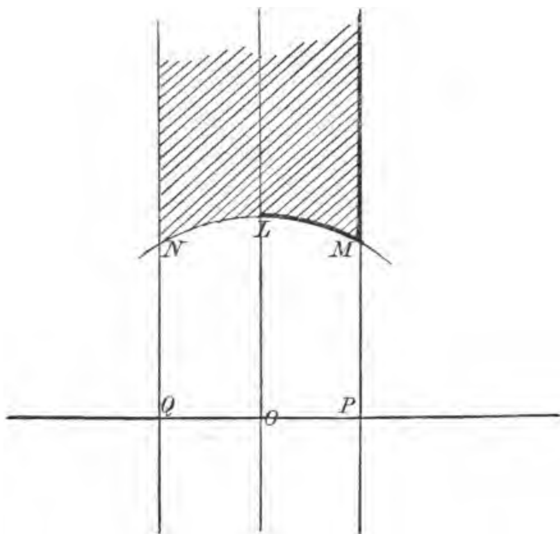


Fig. 7.

welche parallel zur y-Achse im Abstande $\frac{-1}{2}$ von O gezogen ist; den komplexen Werten, für welche $\xi \lesseqgtr \frac{1}{2}$ ist, entsprechen die Punkte auf oder zur Linken der andern Parallelen PM im Abstande $+\frac{1}{2}$ von O, endlich den komplexen Werten, für welche $\xi^2 + \eta^2 \gtreqless 1$ ist, solche Punkte, die außerhalb des Kreises mit dem Mittelpunkte O und dem Radius 1 oder auf seiner Peripherie gelegen sind. Hiernach werden die Punkte, welche den reduzierten Zahlen ω_0 der Gesamtheit Ω entsprechen, wegen der solchen Zahlen charakteristischen Bedingungen (75) in demjenigen Gebiete der Ebene liegen, das in der Figur schraffiert ist, einschließlich des Teils seiner Begrenzung, welcher stärker

ausgezogen ist; indem hierbei der Kreisbogen NL unterdrückt ist, wird der einzige Fall äquivalenter reduzierter Zahlen ausgeschlossen. Da die Anzahl der reduzierten Zahlen nur endlich ist, enthält das bezeichnete Gebiet nur eine endliche Menge von „Bildpunkten“, welche Zahlen ω der Gesamtheit Ω entsprechen. Jeder außerhalb des Gebiets liegende Bildpunkt einer Zahl ω' dieser Gesamtheit aber wird durch eine Substitution

$$\omega = \frac{\alpha\,\omega' + \beta}{\gamma\,\omega' + \delta}$$

der (engeren) linearen Gruppe in einen Punkt dieser endlichen Menge übergeführt.

Stellen wir endlich noch die Bedeutung fest, welche den Reduktionsbedingungen für eine quadratische Form mit Bezug auf das Gitter zukommt, welches die Klasse der Form repräsentiert. Sei dies Gitter das nebenstehende (Fig. 8) mit dem Anfangspunkte O. Um daraus dasjenige

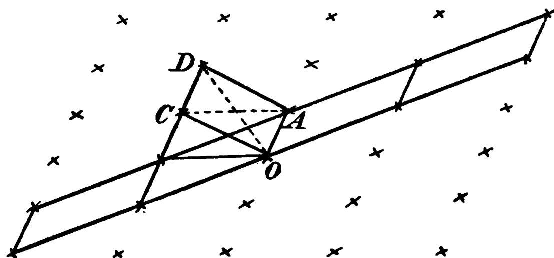


Fig. 8.

Elementarparallelogramm zu ermitteln, welches der reduzierten Form der Klasse entspricht, verbinde man O mit dem nächstgelegenen Gitterpunkte A durch eine Gerade und suche einen derjenigen Gitterpunkte, die in der nächsten Parallelen und O zunächst gelegen sind; sei C solch ein Punkt, dann werden A, C die Grundpunkte für das Gitter der reduzierten Form sein. In der Tat ist die reduzierte Form (a, b, c), da für sie

$$-a < b \lesseqgtr a \lesseqgtr c\,,$$

also $\sqrt{a} \gtreqless \sqrt{c}$ ist, dadurch charakterisiert, daß die Seiten des Elementarparallelogramms $OA \gtreqless OC$, ihre Diagonalen

$$AC = \sqrt{a - b + c}\,, \quad OD = \sqrt{a + b + c}$$

aber zwischen $\sqrt{c}$ und $\sqrt{3c}$ liegen und somit gleich oder größer sind als die Seiten; diese Bedingungen sind aber nur für das angegebene Parallelogramm erfüllt, wie der Anblick der anderen, in der Figur ausgezeichneten Parallelogramme zur Genüge zeigt. Das Elementarparallelogramm der reduzierten Form hat demnach von allen die kleinsten Seiten, und Diagonalen, welche nicht kleiner sind als die Seiten.

18. Wir behandeln nunmehr den Fall einer positiven Diskriminante

$$D > 0\,,$$

sehen dabei aber zunächst davon ab, ob die Äquivalenz eine eigentliche oder uneigentliche sei. Da entgegengesetzte Formen stets — wenigstens uneigentlich — äquivalent sind, kann man den mittleren Koeffizienten der Form so gewählt denken, daß wenigstens eine der beiden Wurzeln

$$(88) \qquad \frac{-b + \sqrt{D}}{2a}\,, \quad \frac{-b - \sqrt{D}}{2a}$$

der Form positiv ist, denn wären beide negativ, so wäre es auch ihre Summe $\frac{-b}{a}$, was nicht der Fall sein wird, wenn b eventuell durch $-b$ ersetzt wird. Betrachten wir also die Gesamtheit Ω der Zahlen (88), in denen a, b ganze Zahlen und $b^2 \equiv D \pmod{4a}$ ist, d. h (vgl. Nr. 13) die Gesamtheit der Wurzeln der quadratischen Formen mit der Diskriminante D, so dürfen wir zur Untersuchung ihrer Äquivalenz von der Annahme ausgehen, daß etwa die Wurzel

$$(89) \qquad \omega = \frac{-b + \sqrt{D}}{2a}$$

positiv sei. Man setze nun $\omega = q_0 + \frac{1}{\omega_1}$, wo q_0 die größte in ω enthaltene ganze Zahl bedeute; dann ist

ω_1 eine positive Irrationalzahl größer als 1. Ebenso setze man

$$\omega_1 = q_1 + \frac{1}{\omega_2}, \quad \omega_2 = q_2 + \frac{1}{\omega_3}, \quad \ldots,$$

unter $q_1, q_2, \ldots$ resp. die größten in $\omega_1, \omega_2, \ldots$ enthaltenen Ganzen verstanden; so entsteht ein Kettenbruch für ω:

(90) $$\omega = \lfloor q_0, q_1, q_2, \ldots, q_{i-1}, \omega_i \rceil,$$

in welchem ω_i wieder eine positive Irrationalzahl größer als 1 bedeutet und der beliebig weit fortgesetzt werden kann. Man bilde die aufeinanderfolgenden Näherungsbrüche dieses Kettenbruchs:

(91) $$\frac{z_0}{n_0} = \frac{1}{0}, \quad \frac{z_1}{n_1} = \frac{q_0}{1}, \quad \frac{z_2}{n_2} = \frac{q_0 q_1 + 1}{q_1}, \quad \frac{z_3}{n_3} = \frac{q_2 z_2 + z_1}{q_2 n_2 + n_1}, \quad \ldots,$$

deren letzter, den Schlußnenner ω_i enthaltender die Gleichung

(92) $$\omega = \frac{z_i \omega_i + z_{i-1}}{n_i \omega_i + n_{i-1}}$$

liefert, welche mit Rücksicht auf die bekannte Beziehung

$$z_i n_{i-1} - n_i z_{i-1} = (-1)^i$$

zwischen den Zählern und Nennern zweier aufeinander folgender Näherungsbrüche die, je nachdem i gerade oder ungerade ist, eigentliche oder uneigentliche Äquivalenz der Zahlen ω, ω_i ausweist. Aus (92) ergibt sich umgekehrt

$$\omega_i = \frac{-n_{i-1}\omega + z_{i-1}}{n_i \omega - z_i}$$

und, da die gleiche Beziehung auch zwischen den konjugierten Werten bestehen muß, die Gleichung

(93) $$\omega_i' = \frac{-n_{i-1}\omega' + z_{i-1}}{n_i \omega' - z_i}.$$

Da nun mit wachsendem h der Bruch $\frac{z_h}{n_h}$ dem Werte ω unendlich nahe kommt, wird von einem bestimmten Werte von h an der Unterschied $\frac{z_h}{n_h} - \omega$ numerisch unter jedem

beliebig gegebenen Werte, z. B. unter $\omega - \omega' = \frac{\sqrt{D}}{a}$ bleiben, und daher der Ausdruck

$$\frac{z_h}{n_h} - \omega + (\omega - \omega') = \frac{z_h}{n_h} - \omega'$$

und, da n_h stets positiv ist, auch der Ausdruck $z_h - n_h \omega'$ dasselbe Vorzeichen behalten wie $\frac{\sqrt{D}}{a}$, d. i. wie a. Für $i > h$ bleibt mithin ω_i' nach Formel (93) stets negativ. Da man diese Formel aber schreiben kann wie folgt:

$$\omega_i' + 1 = \frac{(n_i - n_{i-1})\omega' - (z_i - z_{i-1})}{n_i\left(\omega' - \frac{z_i}{n_i}\right)} = \frac{1}{n_i}\left[n_i - n_{i-1} + \frac{(-1)^{i+1}}{n_i\left(\omega' - \frac{z_i}{n_i}\right)}\right],$$

so ergibt sich, wenn i groß genug gedacht wird, $\omega_i' + 1 > 0$, da $n_i - n_{i-1} \geqq 1$ und der Bruch $\frac{(-1)^{i+1}}{n_i\left(\omega' - \frac{z_i}{n_i}\right)}$ für hinreichend große Werte von i numerisch von $\frac{1}{n_i(\omega' - \omega)}$ beliebig wenig verschieden, mithin beliebig klein ist. Auf solche Weise ist festgestellt, daß für alle hinreichend großen Werte von i jeder Schlußnenner ω_i, der selbst positiv und größer als 1 ist, einen konjugierten Wert ω_i' hat, welcher negativ und numerisch kleiner als 1 ist. Nun gehören sämtliche Zahlen ω_i der Gesamtheit Ω an, denn aus $\omega = q_0 + \frac{1}{\omega_1}$ folgt

$$\omega_1 = \frac{1}{\omega - q_0} = \frac{2a}{-(2aq_0 + b) + \sqrt{D}},$$

was, mit $-(2aq_0 + b) - \sqrt{D}$ erweitert und wenn $b^2 - D = 4ac$ gesetzt wird, mit der Gleichung

$$\omega_1 = \frac{-(2aq_0 + b) - \sqrt{D}}{2(aq_0^2 + bq_0 + c)}$$

übereinkommt und, da

$$(2aq_0 + b)^2 - D = 4(aq_0^2 + bq_0 + c) \cdot a,$$

d. h.

$$(2aq_0 + b)^2 \equiv D \mod. 4(aq_0^2 + bq_0 + c)$$

ist, ω_1 als eine Zahl in Ω ausweist; gleicherweise erkennt man dasselbe für $\omega_2, \omega_3, \ldots$. Nennen wir daher eine Zahl ω_0 der Gesamtheit Ω eine reduzierte Zahl, wenn ω_0 positiv und größer als 1, die ihr konjugierte Zahl ω_0' aber negativ und numerisch kleiner als 1 ist, so dürfen wir als Resultat unserer Betrachtung den Satz aussprechen: Jede (positive) Zahl in Ω ist einer reduzierten Zahl äquivalent.

19. Als eine solche mit ω äquivalente reduzierte Zahl darf jeder Schlußnenner des Kettenbruchs (90) für ein hinreichend großes i angesehen werden. Es gibt deren aber nur eine endliche Anzahl voneinander verschiedener. In der Tat ist die Anzahl der reduzierten Zahlen in Ω selbst nur eine endliche. Soll nämlich

$$\omega_0 = \frac{-b \pm \sqrt{D}}{2a}$$

eine reduzierte Zahl sein, so müssen die folgenden Ungleichheiten

$$0 < \frac{b \pm \sqrt{D}}{2a} < 1 < \frac{-b \pm \sqrt{D}}{2a} \tag{94}$$

erfüllt sein. Aus ihnen folgt nun zunächst $0 < \frac{\pm\sqrt{D}}{a}$, d. h. es gilt das positive oder negative Vorzeichen, je nachdem a positiv oder negativ ist; ist $a > 0$, so nehmen die Ungleichheiten die Form an:

$$0 < b + \sqrt{D} < 2a < -b + \sqrt{D}, \tag{95a}$$

woraus $b < 0$ und $> -\sqrt{D}$ hervorgeht, so daß die ganze Zahl b nur eine endliche Anzahl von Werten haben kann, deren jedem den Ungleichheiten zufolge auch nur eine endliche Anzahl von Werten für die ganze Zahl a entsprechen kann; ist $a < 0$, so lauten die Ungleichheiten:

$$0 > b - \sqrt{D} > 2a > -b - \sqrt{D}, \tag{95b}$$

woraus $b > 0$ und kleiner als $\sqrt{D}$, und somit wieder nur eine endliche Anzahl von zulässigen Werten für b und für a hervorgeht. Zudem dürfen von diesen Wertsystemen nur solche genommen werden, für welche $b^2 \equiv D \pmod{4a}$, d. h. $\frac{b^2 - D}{4a}$ eine ganze Zahl ist. Die Anzahl der für reduzierte

Zahlen ω_0 statthaften Wertsysteme a, b ist also, wie behauptet, nur eine endliche.

Hieraus ist zu schließen, daß, wenn die unendliche Kettenbruchentwicklung für eine positive Zahl ω der Gesamtheit Ω in endlicher Form, wie in (90), geschrieben wird, ihre Schlußnenner ω_i nur eine endliche Anzahl verschiedener Werte haben können, da sie von einer bestimmten endlichen Stelle an reduziert sind. Es muß sich also ereignen, daß einmal ein Schlußnenner einem früheren gleich wird. Sei etwa ω_{i+k} der erste von den auf ω_i folgenden, welcher gleich ω_i ist; dann ist

$$(96)\quad \begin{cases} \omega = \lfloor q_0, q_1, q_2, \ldots, q_{i-1}, \omega_i \rceil \\ \quad = \lfloor q_0, q_1, q_2, \ldots q_{i-1}, q_i, \ldots q_{i+k-1}, \omega_i \rceil \\ \quad = \lfloor q_0, q_1, \ldots q_{i-1}, q_i, \ldots q_{i+k-1}, q_i, \ldots q_{i+k-1}, \omega_i \rceil \end{cases}$$

usw., mit anderen Worten: der Kettenbruch für ω muß periodisch sein.

Man zeigt aber noch leicht, daß die Periode mit dem ersten Schlußnenner ω_i, welcher reduziert ist, beginnt. In einer Formel

$$(97)\qquad \omega_i = q_i + \frac{1}{\omega_{i+1}}$$

mit ganzzahligem q_i ist nämlich dann und nur dann ω_{i+1} zugleich mit ω_i reduziert, wenn q_i das größte in ω_i enthaltene Ganze ist; in der Tat ist unter dieser Voraussetzung ω_{i+1} positiv und größer als 1, und zugleich ist

$$(98)\qquad \omega'_{i+1} = \frac{1}{\omega'_i - q_i},$$

wenn $\omega_i > 1$ und $\omega'_i < 0$ ist, ein negativer echter Bruch, d. h. ω_{i+1} ist reduziert; umgekehrt, wenn ω_{i+1} zugleich mit ω_i reduziert ist, so ist $\frac{1}{\omega_{i+1}}$ positiv und kleiner als 1, also q_i in (97) das größte in dem positiven ω_i enthaltene Ganze; dieselbe Zahl q_i ist dann aber auch das größte Ganze, welches in $\frac{-1}{\omega'_{i+1}}$ enthalten ist, denn aus (98) folgt

$$\frac{-1}{\omega'_{i+1}} = q_i - \omega'_i,$$

worin $-\omega_i'$ ein positiver echter Bruch ist. — Dies vorausgeschickt, nehme man an, daß die Periodizität des Kettenbruchs für ω erst mit dem Schlußnenner ω_{i+1} beginne, der nicht der erste reduzierte Schlußnenner ist, und es sei $\omega_{k+i+1} = \omega_{i+1}$. Dann bestehen Gleichungen von der Form

$$\omega_i = q_i + \frac{1}{\omega_{i+1}}, \qquad \omega_{i+k} = q_{i+k} + \frac{1}{\omega_{i+k+1}} = q_{i+k} + \frac{1}{\omega_{i+1}},$$

wo q_i, q_{i+k} die größten in ω_i und ω_{i+k} enthaltenen Ganzen bezeichnen. Da aber $\omega_i, \omega_{i+1}, \omega_{i+k}$ reduziert sind, muß dem soeben Bewiesenen zufolge sowohl q_i als auch q_{i+k} das größte in $\frac{-1}{\omega_{i+1}'}$ enthaltene Ganze und somit $q_i = q_{i+k}$ sein, die Periodizität nähme also gegen die Voraussetzung bereits um eine Stelle früher beim Schlußnenner ω_i ihren Anfang. Auf solche Weise sind wir zu folgendem **Satze** gelangt:

Jede (positive) ganze Zahl ω der Gesamtheit Ω läßt sich in einen periodischen Kettenbruch entwickeln, dessen Periode bei dem ersten Schlußnenner beginnt, welcher reduziert ist.

Ist demnach ω_0 eine reduzierte Zahl in Ω, so beginnt die Periodizität schon mit ω_0 selbst, d. h. die Kettenbruchentwicklung von ω_0 ist rein periodisch:

$$\omega_0 = \lfloor q_0, q_1, \ldots, q_{k-1}, q_0, q_1, \ldots, q_{k-1}, q_0, \ldots \rceil$$

oder, wie wir kürzer schreiben wollen,

(99) $$\omega_0 = K(q_0, q_1, \ldots, q_{k-1}).$$

20. Durch die Kettenbruchentwicklung einer reduzierten Zahl ω_0 wird nun eine Anzahl reduzierter Zahlen, nämlich die endliche Menge der Schlußnenner

(100) $$\omega_0, \omega_1, \omega_2, \ldots, \omega_{k-1}$$

des Kettenbruchs für ω_0, zu einer Periode untereinander äquivalenter Zahlen verbunden, deren Kettenbruchentwicklungen aus (99) durch einfache Verschiebung der Teilnenner hervorgehen, nämlich:

$$\omega_1 = K(q_1, q_2, \ldots, q_{k-1}, q_0)$$
$$\omega_2 = K(q_2, q_3, \ldots, q_0, q_1)$$
$$\cdots\cdots\cdots\cdots$$
$$\omega_{k-1} = K(q_{k-1}, q_0, \ldots, q_{k-3}, q_{k-2}),$$

während die Gleichungen

$$\omega_0 = q_0 + \frac{1}{\omega_1},\ \omega_1 = q_1 + \frac{1}{\omega_2},\ \ldots,\ \omega_{k-1} = q_{k-1} + \frac{1}{\omega_0}$$

zeigen, daß jede dieser Zahlen der ihr vorhergehenden wie der ihr folgenden uneigentlich äquivalent ist, da z. B. ω_{i-1} aus ω_i durch die Substitution S_{i-1}:

$$\omega_{i-1} = \frac{q_{i-1}\cdot\omega_i + 1}{1\cdot\omega_i + 0}$$

mit der Determinante $q_{i-1}\cdot 0 - 1\cdot 1 = -1$ entsteht. Erschöpft nun die Periode (100) noch nicht die Gesamtheit der reduzierten Zahlen in Ω, so sei $\overline{\omega}_0$ eine der noch übrigen; ihre Kettenbruchentwicklung liefert eine zweite Periode

(101) $$\overline{\omega}_0,\ \overline{\omega}_1,\ \overline{\omega}_2,\ \ldots\ \overline{\omega}_{\bar{k}-1}$$

von untereinander äquivalenten reduzierten Zahlen, und wenn auch hiermit noch deren Menge nicht erschöpft ist, kann man in gleicher Weise fortfahren und erhält endlich sämtliche reduzierten Zahlen in Ω in eine gewisse Anzahl solcher Perioden verteilt. Während aber die Glieder jeder einzelnen Periode untereinander äquivalent sind, können zwei Zahlen verschiedener Perioden einander nicht äquivalent, also a fortiori auch nicht einander gleich sein. Denn die Kettenbruchentwicklungen für äquivalente Zahlen stimmen einem früheren Satze (Kap. 4, Nr. 14) zufolge von einer bestimmten Stelle ab miteinander, also auch in ihren Schlußnennern, überein, welche somit ein und dieselbe Periode darstellen müßten, der Voraussetzung zuwider. Somit stellen die gedachten Perioden die Gesamtheit der verschiedenen reduzierten Zahlen in Ω und zugleich ihre Verteilung in Klassen äquivalenter reduzierter Zahlen dar. Die Anzahl dieser Klassen ist endlich, da es die Anzahl der reduzierten Zahlen selbst ist; man erkennt also, wenn man von den Zahlen zu den ihnen entsprechenden quadratischen Formen zurückkehrt, daß auch bei positiver Diskriminante die Anzahl Klassen äquivalenter quadratischer Formen nur endlich ist.

Hiermit sind wir nun auch für den Fall positiver Diskriminante in den Stand gesetzt, die Frage nach der Äquivalenz

zweier Zahlen in Ω oder der ihnen entsprechenden quadratischen Formen zu entscheiden. Jede der gedachten beiden Zahlen ist (nach Nr. 18) je einer reduzierten Zahl äquivalent, je nachdem aber diese letzteren Zahlen derselben oder verschiedenen Perioden angehörig sind, werden die gegebenen Zahlen einander äquivalent sein oder nicht. Die Kettenbrüche zweier äquivalenter Zahlen sind also dadurch charakterisiert, daß sie von dem ersten bei ihnen auftretenden reduzierten Schlußnenner an die gleiche Periode von Schlußnennern ergeben, und können abgesehen von dem anfänglichen Teile nur darin untereinander verschieden sein, daß die Periode beidemal mit einem andern ihrer Glieder einsetzt. Ist z. B. für eine dieser Zahlen dies Glied das erste Glied ω_0 der Periode (100), für die andere Zahl das Glied ω_i, so kann auch leicht entschieden werden, ob die Äquivalenz der beiden Zahlen die eigentliche oder die uneigentliche ist. Da nämlich jede der Zahlen (100) der folgenden uneigentlich äquivalent ist, wird sie der jedesmal zweitfolgenden eigentlich äquivalent und somit ω_0 mit ω_i eigentlich oder uneigentlich äquivalent sein, je nachdem i gerade oder ungerade ist. Nun bestimmt sich (nach Nr. 18) aus den anfänglichen Teilen der Kettenbrüche der beiden gegebenen Zahlen, welcher Art ihre Äquivalenz mit ω_0 bzw. mit ω_i ist; wenn sie beidemal von gleicher Art ist, so werden die Zahlen auch untereinander von eben dieser Art oder aber von der entgegengesetzten Art äquivalent sein, je nachdem i gerade oder ungerade ist; wenn dagegen ihre Äquivalenz mit ω_0 bzw. mit ω_i von verschiedener Art ist, werden sie untereinander, je nachdem i gerade oder ungerade ist, uneigentlich oder eigentlich äquivalent sein.

Zugleich liefern die Kettenbruchentwicklungen äquivalenter Zahlen auch eine Substitution, durch welche die eine von ihnen in die andere übergeht. Aus der Formel (96) findet sich offenbar, daß ω aus ω_i durch die zusammengesetzte Substitution

$$S_0 \cdot S_1 \ldots S_{i-1}$$

hervorgeht. Da aber die Kettenbrüche äquivalenter Zahlen dieselbe Periode von Schlußnennern aufweisen, tritt ω_i auch im Kettenbruche der mit ω äquivalenten Zahl als Schlußnenner auf, und es ergibt sich aus ihm eine analoge Substitution, durch welche diese Zahl aus ω_i, also auch umgekehrt

eine Substitution, durch welche ω_i aus jener hervorgeht. Durch Zusammensetzung der erstgenannten Substitution und dieser letzteren entsteht aber ω unmittelbar aus der ihr äquivalenten Zahl.

21. Übertragen wir diese Betrachtungen von den Zahlen der Gesamtheit Ω auf die ihnen entsprechenden Formen mit der Diskriminante D, so sehen wir an die Stelle der Perioden reduzierter Zahlen Perioden reduzierter Formen treten, auf welche wir noch einen Augenblick näher eingehen wollen. Wir nennen eine Form (a, b, c) reduziert, wenn eine ihrer Wurzeln, etwa

$$\omega_0 = \frac{-b+\sqrt{D}}{2a},$$

eine reduzierte Zahl ist. Stellt man sich die reellen Werte als Punkte einer Geraden dar, so wird die Lage der

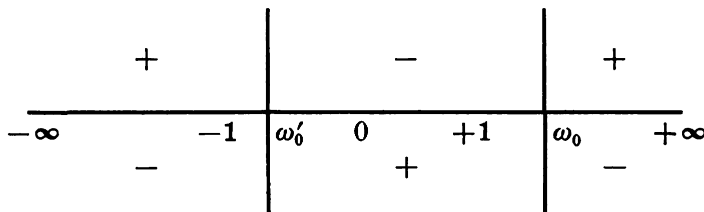


Fig. 9.

Wurzeln ω_0, ω_0' auf derselben durch nebenstehende Fig. 9 gekennzeichnet. Da nun ω_0, ω_0' die Wurzeln der Gleichung

$$az^2 + bz + c = 0$$

sind, wird das Vorzeichen des Ausdrucks $az^2 + bz + c$ für die einzelnen Abschnitte der unendlichen Geraden, denen der Wert von z entspricht, bei positivem a das oberhalb, bei negativem a das unterhalb der Geraden angegebene Zeichen sein. Der $z = 1$ entsprechende Wert

$$a + b + c$$

wird daher im ersteren Falle negativ, im zweiten Falle positiv sein. Nehmen wir der Bestimmtheit wegen $a > 0$ an, was ein negatives c zur Folge hat, da ω_0, ω_0' entgegengesetztes Vorzeichen haben, und machen in der Form

$$f_0 = ax^2 + bxy + cy^2$$

die Transformation T:

$$x = x' + y', \quad y = y',$$

so geht sie über in die Form

$$f_0^{(1)} = a x'^2 + (2a + b) x' y' + (a + b + c) y'^2$$
$$= (a, 2a + b, a + b + c),$$

in welcher nach der Vorbemerkung der dritte Koeffizient $a + b + c < 0$ ist; ihre erste Wurzel ist

$$\omega_0^{(1)} = \frac{-(2a + b) + \sqrt{D}}{2a} = \omega_0 - 1,$$

also positiv, während die zweite Wurzel

$$\omega_0'^{(1)} = \omega_0' - 1$$

negativ und numerisch größer als 1 ist. Wird nun q_0 in der Gleichung $\omega_0 = q_0 + \frac{1}{\omega_1}$ größer als 1 gedacht, so liegt $\omega_0^{(1)}$ noch zur Rechten des Punktes 1 und man schließt daher, daß die Summe der Koeffizienten der Form d. i.

$$4a + 2b + c < 0$$

ist. Bei wiederholter Anwendung der Transformation T entsteht die Form

$$f_0^{(2)} = (a, 4a + b, 4a + 2b + c),$$

deren dritter Koeffizient noch negativ ist, während ihre erste Wurzel $\omega_0^{(2)} = \omega_0^{(1)} - 1 = \omega_0 - 2$ positiv und, wenn $q_0 > 2$ gedacht wird, noch größer als 1 ist, die zweite Wurzel $\omega_0'^{(2)} = \omega_0' - 2$ dagegen negativ und numerisch größer als 1 ist. Somit wird die Summe $9a + 3b + c$ der drei Koeffizienten noch negativ sein. So kann man fortfahren, solange die erste Wurzel der neuen Form noch größer als 1 bleibt, d. h. bis zur Form

$$f_0^{(q_0)} = (a, 2q_0 a + b, q_0^2 a + q_0 b + c), \tag{102}$$

in welcher der letzte Koeffizient noch negativ, die erste Wurzel $\omega_0^{(q_0)} = \omega_0 - q_0$ nun aber kleiner als 1 ist, die Summe der drei Koeffizienten also positiv. Die so entstandenen Formen sind nicht reduziert, da ihre zweite Wurzel zwar negativ, aber numerisch größer als 1 ist.

Der bisherige Fortgang entspricht dem ersten Gliede des Kettenbruchs

(103) $$\omega_0 = K(q_0, q_1, q_2, \ldots, q_{k-1}).$$

Machen wir nun aber der Formel $\omega_0 = q_0 + \frac{1}{\omega_1}$ gemäß die Substitution $\omega_0^{(q_0)} = \frac{1}{\omega_1}$, und wenden die ihr entsprechende Transformation

$$x = y', \quad y = x'$$

auf die Form (102) an, so entsteht die Form

$$f_1 = (a_1, b_1, c_1) = (q_0^2 a + q_0 b + c, 2 q_0 a + b, a),$$

welche wieder reduziert ist, da ihre Wurzel ω_1 reduziert, nämlich das zweite Glied der Periode (100) ist, als deren erstes ω_0 gedacht worden ist. In dieser Form ist aber jetzt der erste Koeffizient a_1 negativ, der dritte c_1 positiv, die Verteilung der Vorzeichen in der zugehörigen Figur also die in obiger Figur unterhalb angegebene, und daher die Summe der drei Koeffizienten:

$$a_1 + b_1 + c_1 > 0.$$

Wenn nun aufs neue zu wiederholten Malen die Transformation T angewandt wird, so entsteht dem zweiten Gliede q_1 des Kettenbruchs (103) entsprechend eine Reihe nicht reduzierter Formen

$$f_1^{(1)} = (a_1, \quad 2 a_1 + b_1, \quad a_1 + b_1 + c_1)$$
$$f_1^{(2)} = (a_1, \quad 4 a_1 + b_1, \quad 4 a_1 + 2 b_1 + c_1)$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$f_1^{(q_1)} = (a_1, \quad 2 q_1 a_1 + b_1, \quad q_1^2 a_1 + q_1 b_1 + c_1),$$

in welchen der letzte Koeffizient noch positiv ist, während nach der Formel $\omega_1 = q_1 + \frac{1}{\omega_2}$ die Wurzel $\omega_1^{(q_1)}$ der letzten zwar noch positiv, aber kleiner als 1, die Summe der drei Koeffizienten mithin nicht mehr positiv ist. Die Substitution $\omega_1^{(q_1)} = \frac{1}{\omega_2}$ oder die ihr entsprechende Transformation

$$x = y', \quad y = x'$$

verwandelt dann $f_1^{(q_1)}$ in die reduzierte Form

$$f_2 = (a_2, b_2, c_2) = (q_1^2 a_1 + q_1 b_1 + c_1, 2 q_1 a_1 + b_1, a_1)$$

mit der Wurzel ω_2 (dem dritten Gliede der Periode (100)) und einem positiven ersten Koeffizienten a_2, und man kann nun mit f_2 fortfahren, wie man mit f_0 begonnen hat, und erhält auf diese Weise die gesamte Periode

$$f_0, f_1, f_2, \ldots, f_{k-1}$$

der der Periode (100) entsprechenden reduzierten Formen.

Bedenkt man, daß die Transformation $x = y'$, $y = x'$, welche von $f_0^{(q_0)}$ zu f_1 führt, nur eine Vertauschung der Unbestimmten der Form bedeutet, so leuchtet ein, daß die wiederholte Ausführung der Transformation T an der Form f_1 dasselbe ist, wie diejenige der Transformation T':

$$x = x', \quad y = x' + y'$$

an der Form $f_0^{(q_0)}$. Daher läßt sich das Ergebnis der voraufgehenden Betrachtung auch folgendermaßen fassen:

Wenn auf die reduzierte Form (a, b, c), deren erster Koeffizient a positiv gedacht wird, die Transformation T so oft ausgeführt wird, als der dritte Koeffizient der entstehenden Formen noch negativ bleibt, dann die Transformation T' so oft, als der erste Koeffizient der dann entstehenden Formen noch positiv bleibt, dann wieder nach derselben Regel die Transformation T usw., so bilden die bei dem jedesmaligen Übergange von der Transformation T zur Transformation T' und umgekehrt entstehenden Formen die Periode reduzierter Formen, welcher die Form f_0 angehört, und die Zahlen $q_0, q_1, q_2, \ldots$, welche angeben, wie oft die Transformationen $T, T', T, \ldots$ angewandt werden müssen, die Periode des Kettenbruchs für die erste Wurzel der Form f_0.

22. Was endlich die geometrische Deutung der Reduktion anbelangt, so ist sie für den Fall einer positiven Diskriminante eine wesentlich andere, wie für den einer negativen. Doch müssen wir uns hier darauf beschränken, die Figur anzugeben, welche an die Stelle der Fig. 7 für den letzteren Fall (in Nr. 17) tritt, und im übrigen den Leser auf *F. Kleins* autographierte Vorlesungshefte (Ausgewählte Kapitel der Zahlentheorie I) verweisen, wo er auch eine, von *H. Hurwitz* (Mathem. Annalen Bd. 45) schön entwickelte andere geometrische Auffassung der Reduktion quadratischer Formen für positive sowohl wie für negative Diskriminanten findet, welche

in einem höheren Gebiete der Analysis von ganz besonderer Bedeutung ist.

Setzt man in einer Zahl $\omega = \frac{-b + \varepsilon\sqrt{D}}{2a}$ der Gesamtheit Ω, wo $\varepsilon = \pm 1$ gedacht ist, $\frac{-b}{2a} = x$, $\frac{\varepsilon}{2a} = y$ und faßt x, y als rechtwinklige Koordinaten eines Punktes in einer Ebene auf (Fig. 10), so wird jeder Zahl der Gesamtheit Ω

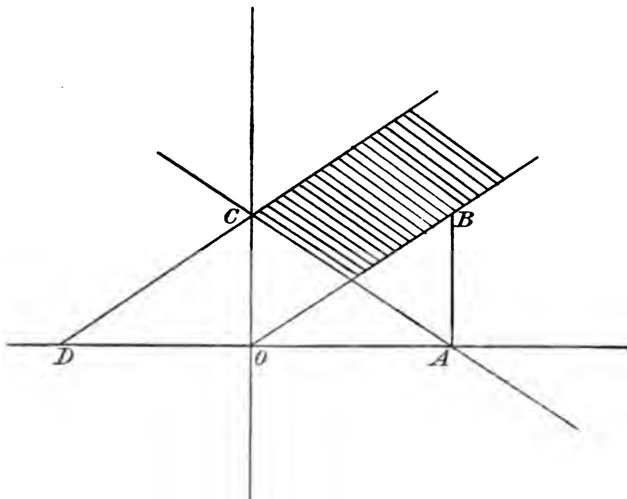


Fig. 10.

ein bestimmter Punkt der Ebene zugeordnet sein, der als ihr Bildpunkt aufgefaßt werden kann. Ist nun $OA = 1$, $AB = OC = \frac{1}{\sqrt{D}}$, so haben die drei Geraden OB, CA und die zur ersteren durch C gehende Parallele DC in laufenden Koordinaten u, v die drei Gleichungen:

$$v = \frac{1}{\sqrt{D}} \cdot u, \qquad v = \frac{-1}{\sqrt{D}}(u-1), \qquad v = \frac{1}{\sqrt{D}}(u+1)$$

resp.; da für eine reduzierte Zahl ω die Bedingungen

$$0 < \frac{b + \varepsilon\sqrt{D}}{2a} < 1 < \frac{-b + \varepsilon\sqrt{D}}{2a},$$

für den ihr entsprechenden Punkt x, y der Ebene also die Ungleichheiten

$$0 < -x + y\sqrt{D} < 1 < x + y\sqrt{D}$$

bestehen, so liegt von O aus gesehen dieser Punkt einerseits links von OB und jenseits CA, andererseits diesseits DC, mithin in dem in der Figur schraffierten Parallelstreifen der Ebene, und umgekehrt sind die Zahlen der Gesamtheit Ω, welche durch Punkte dieses Streifens abgebildet werden, reduziert. Die Anzahl solcher Punkte ist daher nur endlich, und sie können so in Systeme zusammengestellt werden, daß die Punkte eines Systems durch Substitutionen der (engeren) linearen Gruppe ineinander übergeführt werden können, zwei Punkte verschiedener Systeme aber nicht. Jeder außerhalb des Streifens gelegene Bildpunkt einer Zahl ω aber wird durch solche Substitutionen in die Punkte eines einzigen ganz bestimmten jener Systeme übergeführt.

Zweiter Abschnitt.

Der quadratische Zahlenkörper.

Erstes Kapitel.

Zahlen, Moduln, Ideale des Körpers.

1. In den letzten Nummern des vorigen Abschnittes haben wir das Gebiet des rationalen Zahlenkörpers überschritten und Zahlen in Betracht gezogen, die aus einer Irrationalität, der Quadratwurzel aus D, auf rationale Weise gebildet sind. Es hat sich aus unseren Betrachtungen ergeben, in wie innigem Zusammenhange die Eigenschaften solcher Zahlen mit der Theorie der quadratischen Formen stehen, ein Umstand, den schon die Zerlegung dieser Formen in zwei irrationale Linearfaktoren oder die Einführung der Gitterzahlen erkennen ließ. So werden wir naturgemäß zur näheren Betrachtung solcher Zahlen an sich gedrängt und werden aus derselben ersehen, daß deren Theorie den eigentlich arithmetischen Kern der Lehre von den quadratischen Formen ausmacht.

Man nennt algebraische Zahl jede Zahl ω, welche einer algebraischen Gleichung

$$(1) \qquad a_0 z^n + a_1 z^{n-1} + a_2 z^{n-2} + \ldots + a_{n-1} z + a_n = 0$$

mit ganzzahligen Koeffizienten genügt; ist dies die Gleichung kleinsten Grades von dieser Beschaffenheit, welche ω erfüllt, so heißt ω eine algebraische Zahl vom Grade n, und sie wird eine ganze algebraische — oder, wo kein Mißverständnis zu befürchten ist, kurz eine ganze Zahl dieses Grades genannt, wenn der Koeffizient a_0 der höchsten Potenz von z gleich Eins ist.

Hiernach ist, wenn auch fernerhin unter d eine ganze Zahl von derselben Art wie im vorigen Abschnitte verstanden wird, die Zahl

(2) $$\delta = \sqrt{d}$$

eine ganze Zahl zweiten Grades, da sie der Gleichung

(3) $$z^2 = d\,,$$

aber als irrationaler Wert keiner Gleichung ersten Grades genügt. Da nun jede gerade Potenz von δ,

$$\delta^{2h} = d^h\,,$$

eine ganze rationale Zahl, jede ungerade Potenz

$$\delta^{2h+1} = d^h \cdot \sqrt{d}$$

aber das Produkt einer ganzen Zahl in $\sqrt{d}$ ist, so wird jede ganze Funktion von δ mit ganzzahligen Koeffizienten offenbar auf die Form $r' + s' \cdot \sqrt{d}$ gebracht werden können, in welcher r', s' ganze rationale Zahlen bedeuten, jede rationale Funktion von δ mit ganzzahligen Koeffizienten also auf die Form

$$\frac{r' + s'\sqrt{d}}{r'' + s''\sqrt{d}}\,,$$

wo auch r'', s'' ganze Zahlen bedeuten, ein Ausdruck, dem jedoch durch Erweiterung mit $r'' - s''\sqrt{d}$ die Gestalt

$$\frac{(r' + s'\sqrt{d})(r'' - s''\sqrt{d})}{r''^2 - s''^2 \cdot d} = \frac{r'r'' - ds's'' + (r''s' - r's'')\sqrt{d}}{r''^2 - ds''^2}\,,$$

d. h. die Gestalt

(4) $$\frac{r + s\sqrt{d}}{t}$$

gegeben wird, wo nun

$$r = r'r'' - ds's''\,, \qquad s = r''s' - r's''\,, \qquad t = r''^2 - ds''^2$$

wieder ganze rationale Zahlen sind. Jede Zahl also, welche aus $\sqrt{d}$ auf rationale Weise hervorgebracht werden kann, hat die Form (4).

Seien
$$\frac{r' + s'\sqrt{d}}{t'}\,, \qquad \frac{r'' + s''\sqrt{d}}{t''}$$

zwei solche Zahlen; man darf voraussetzen, daß ihre Nenner gleich sind, da man andernfalls dies erreichen könnte, indem man die erste mit t'', die zweite mit t' erweiterte; sei also t der gemeinsame Nenner. Dann sieht man ohne weiteres, daß Summe und Differenz beider Zahlen wieder eine Zahl derselben Gestalt ist; desgleichen ihr Produkt

$$\frac{r' + s'\sqrt{d}}{t} \cdot \frac{r'' + s''\sqrt{d}}{t} = \frac{r'r'' + ds's'' + (r's'' + r''s')\sqrt{d}}{t^2};$$

endlich kann aber auch ihr Quotient

$$\frac{r' + s'\sqrt{d}}{r'' + s''\sqrt{d}},$$

wie vorher gezeigt, auf dieselbe Gestalt gebracht werden. Die Gesamtheit der Zahlen, welche auf rationale Weise aus $\sqrt{d}$ entstehen, hat also die Eigenschaft, daß Summe, Differenz, Produkt und Quotient von je zwei ihrer Zahlen, gleichviel ob diese identisch oder verschieden sind, wieder eine Zahl derselben Gesamtheit ist, d. h. sie ist ein Zahlenkörper. Wir bezeichnen diesen durch das Zeichen $\mathfrak{K}(\sqrt{d})$ oder kürzer durch $\mathfrak{K}$ und nennen ihn, da die ihn erzeugende Zahl $\sqrt{d}$, wie bemerkt, eine algebraische Zahl zweiten Grades ist, ebenfalls einen Körper vom zweiten Grade oder einen quadratischen Zahlenkörper.

2. Dieser Körper $\mathfrak{K}$ enthält den rationalen Zahlenkörper $\mathfrak{R}$, denn alle rationalen Zahlen gehen aus (4) hervor, wenn $s = 0$ gedacht wird. Alle übrigen Zahlen in $\mathfrak{K}$ aber sind algebraische Zahlen zweiten Grades. Setzt man nämlich

$$\omega = \frac{r + s\sqrt{d}}{t},$$

so folgt $(t\omega - r)^2 = ds^2$ oder

$$(5) \qquad t^2\omega^2 - 2tr\omega + r^2 - ds^2 = 0,$$

mithin ist ω Wurzel einer ganzzahligen quadratischen Gleichung, und da ω nur rational sein kann, wenn $s = 0$, ist anderenfalls diese Gleichung auch die niedrigste ganzzahlige Gleichung, der ω genügt. Nennt man die Zahl

$$\omega' = \frac{r - s\sqrt{d}}{t},$$

welche aus ω durch Veränderung des Vorzeichens von $\sqrt{d}$ entsteht, d. h. die zweite Wurzel der Gleichung (5) die zu ω konjugierte Zahl, so ist auch diese eine Zahl des Körpers $\mathfrak{K}$. Das Produkt der beiden konjugierten Zahlen ω, ω' heißt die Norm jeder von ihnen, in Zeichen:

$$(6) \qquad N(\omega) = N(\omega') = \omega \cdot \omega' ;$$

sie ist stets eine rationale Zahl; in der Tat ist das Produkt der beiden Wurzeln der Gleichung (5) gleich $\frac{r^2 - ds^2}{t^2}$. Die zu einer rationalen Zahl $\frac{r}{t}$ konjugierte Zahl ist offenbar ihr selbst gleich und demnach ihre Norm gleich ihrem Quadrate.

Wir nennen Zahlen $\omega, \omega_1, \omega_2, \ldots$ des Körpers $\mathfrak{K}$ unabhängig voneinander, wenn eine Gleichung

$$\varrho\,\omega + \varrho_1\,\omega_1 + \varrho_2\,\omega_2 + \ldots = 0,$$

in welcher die Koeffizienten $\varrho, \varrho_1, \varrho_2, \ldots$ rational gedacht sind, nicht anders bestehen kann, als wenn diese Koeffizienten sämtlich Null sind. Damit zwei Zahlen

$$\omega_1 = \frac{r_1 + s_1\sqrt{d}}{t}, \qquad \omega_2 = \frac{r_2 + s_2\sqrt{d}}{t},$$

deren Nenner gleich gedacht werden dürfen, unabhängig voneinander sind, ist notwendig und hinreichend, daß $r_1 s_2 - r_2 s_1$ von Null verschieden ist. In der Tat ist dies hinreichend, denn die Gleichung

$$(7) \qquad \varrho_1\,\omega_1 + \varrho_2\,\omega_2 = 0,$$

d. h. die beiden Gleichungen

$$\varrho_1 r_1 + \varrho_2 r_2 = 0, \qquad \varrho_1 s_1 + \varrho_2 s_2 = 0,$$

aus denen sich

$$(r_1 s_2 - r_2 s_1)\,\varrho_1 = 0 \quad \text{und} \quad (r_1 s_2 - r_2 s_1)\,\varrho_2 = 0$$

ergeben, können für nicht verschwindende ϱ_1, ϱ_2 nur bestehen, wenn $r_1 s_2 - r_2 s_1 = 0$ ist. Es ist aber auch notwendig, denn, ist im Gegenteil $r_1 s_2 - r_2 s_1 = 0$, d. h. $r_1 s_2 = r_2 s_1$, so schließt man, wenn τ_1 den größten gemeinsamen Teiler von r_1, s_1 bezeichnet, so daß $r_1 = \tau_1 r$, $s_1 = \tau_1 s$

und r, s teilerfremd sind, die Gleichungen $r_2 = \tau_2 r$, $s_2 = \tau_2 s$, wo τ_2 eine ganze Zahl bezeichnet, mithin

$$\omega_1 = \tau_1 \omega\,, \qquad \omega_2 = \tau_2 \omega\,,$$

wenn $\omega = \frac{r + s\sqrt{d}}{t}$ gedacht wird, und somit besteht die Gleichung (7) für die nicht verschwindenden Werte $\varrho_1 = \tau_2$, $\varrho_2 = -\tau_1$.

Hieraus folgt sogleich, daß je drei Zahlen in $\mathfrak{K}$:

$$\omega = \frac{r + s\sqrt{d}}{t}\,, \qquad \omega_1 = \frac{r_1 + s_1\sqrt{d}}{t}\,, \qquad \omega_2 = \frac{r_2 + s_2\sqrt{d}}{t}\,,$$

die wir wieder mit gleichem Nenner schreiben, stets voneinander abhängig sind. In der Tat wird die Gleichung

$$\varrho\,\omega + \varrho_1\,\omega_1 + \varrho_2\,\omega_2 = 0\,,$$

falls ω_1, ω_2 voneinander abhängig sind, durch $\varrho = 0$ und nicht verschwindende Werte von ϱ_1, ϱ_2 erfüllt; sind dagegen ω_1, ω_2 voneinander unabhängig, so können rationale Zahlen ϱ_1, ϱ_2 so gewählt werden, daß

$$\omega = \varrho_1\,\omega_1 + \varrho_2\,\omega_2$$

wird, d. h. daß die Gleichungen

$$r = \varrho_1 r_1 + \varrho_2 r_2\,, \qquad s = \varrho_1 s_1 + \varrho_2 s_2$$

befriedigt werden, denn die Determinante $r_1 s_2 - r_2 s_1$ dieser Gleichungen ist dann verschieden von Null. So ist der wichtige **Satz** festgestellt:

Sind ω_1, ω_2 irgend zwei voneinander unabhängige Zahlen in $\mathfrak{K}$, so kann jede Zahl ω dieses Körpers in der Form

$$\omega = \varrho_1\,\omega_1 + \varrho_2\,\omega_2 \tag{8}$$

mit rationalen Koeffizienten ϱ_1, ϱ_2 dargestellt werden. Auch ist solche Darstellung eine völlig eindeutige; denn, wäre auch

$$\omega = \varrho_1'\,\omega_1 + \varrho_2'\,\omega_2\,,$$

so folgte

$$(\varrho_1 - \varrho_1')\,\omega_1 + (\varrho_2 - \varrho_2')\,\omega_2 = 0\,,$$

da aber ω_1, ω_2 unabhängig sind, müßten $\varrho_1 = \varrho_1'$, $\varrho_2 = \varrho_2'$ sein. Man nennt in Anbetracht dieses Satzes je zwei unabhängige Zahlen ω_1, ω_2 des Körpers $\mathfrak{K}$ eine Basis des Körpers.

Die ursprüngliche Darstellung (4) ist nur ein spezieller Fall dieses Ergebnisses, denn, weil eine Gleichung

$$1 \cdot \varrho_1 + \varrho_2 \cdot \sqrt{d} = 0$$

mit rationalen, nicht verschwindenden ϱ_1, ϱ_2 unmöglich ist, sind 1, $\sqrt{d}$ zwei unabhängige Zahlen in $\mathfrak{K}$ und jede Zahl ω des Körpers hat die Gestalt

$$\omega = \frac{r}{t} \cdot 1 + \frac{s}{t} \cdot \sqrt{d}\,.$$

Hiernach kann die Basis des Körpers $\mathfrak{K}$ sehr verschieden gewählt werden, doch ist die Beziehung zwischen den verschiedenen Basen sehr einfach. Sind nämlich wieder ω_1, ω_2 eine solche und

$$(9) \qquad \xi_1 = \sigma_1 \omega_1 + \sigma_2 \omega_2\,, \qquad \xi_2 = \tau_1 \omega_1 + \tau_2 \omega_2$$

zwei Zahlen in $\mathfrak{K}$, so werden auch ξ_1, ξ_2 eine Basis des Körpers $\mathfrak{K}$ sein oder nicht, je nachdem die Determinante $\sigma_1 \tau_2 - \sigma_2 \tau_1$ von Null verschieden oder gleich Null ist. Denn aus (9) folgen die Gleichungen

$$(10) \qquad \begin{cases} (\sigma_1 \tau_2 - \sigma_2 \tau_1) \cdot \omega_1 = \tau_2 \xi_1 - \sigma_2 \xi_2 \\ (\sigma_1 \tau_2 - \sigma_2 \tau_1) \cdot \omega_2 = -\tau_1 \xi_1 + \sigma_1 \xi_2\,; \end{cases}$$

ist nun $\sigma_1 \tau_2 - \sigma_2 \tau_1 = 0$, so besteht zwischen ξ_1, ξ_2 eine lineare Beziehung mit nicht verschwindenden Koeffizienten und somit bilden sie keine Basis des Körpers; hingegen sind sie eine solche, wenn $\sigma_1 \tau_2 - \sigma_2 \tau_1$ von Null verschieden ist, denn dann nehmen durch Division mit $\sigma_1 \tau_2 - \sigma_2 \tau_1$ die Gleichungen (10) die Gestalt an:

$$\omega_1 = \sigma_1' \xi_1 + \sigma_2' \xi_2\,, \qquad \omega_2 = \tau_1' \xi_1 + \tau_2' \xi_2$$

mit rationalen Koeffizienten, und jede Zahl ω des Körpers kann, weil in der Gestalt $\omega = \varrho_1 \omega_1 + \varrho_2 \omega_2$ darstellbar, auch durch die Formel

$$\omega = (\varrho_1 \sigma_1' + \varrho_2 \tau_1')\, \xi_1 + (\varrho_1 \sigma_2' + \varrho_2 \tau_2')\, \xi_2$$

mit rationalen Koeffizienten dargestellt werden.

Man kommt von hier auf die oben gegebene Bedingung für zwei unabhängige Zahlen ω_1, ω_2 wieder zurück, wenn man von der besonderen Basis 1, $\sqrt{d}$ ausgeht.

Sind nun

$$\omega_1 = \frac{r_1 + s_1\sqrt{d}}{t}, \qquad \omega_2 = \frac{r_2 + s_2\sqrt{d}}{t}$$

eine Basis von $\mathfrak{K}$, so sind es die konjugierten Zahlen

$$\omega_1' = \frac{r_1 - s_1\sqrt{d}}{t}, \qquad \omega_2' = \frac{r_2 - s_2\sqrt{d}}{t}$$

jener Bedingung gemäß ersichtlich auch. Aus diesen Formeln folgt

$$\omega_1\omega_2' - \omega_2\omega_1' = \frac{-2(r_1 s_2 - r_2 s_1)\sqrt{d}}{t^2},$$

mithin

(11) $$(\omega_1\omega_2' - \omega_2\omega_1')^2 = \frac{4(r_1 s_2 - r_2 s_1)^2 \cdot d}{t^4}.$$

Der so gebildete Ausdruck heiße die Diskriminante der Basis ω_1, ω_2 und werde mit $\Delta(\omega_1, \omega_2)$ bezeichnet; sie ist stets eine rationale Zahl.

3. Wir richten nun unsere Aufmerksamkeit insbesondere auf die (algebraisch) ganzen Zahlen des Körpers $\mathfrak{K}$. Um sie aus demselben auszusondern, hat man zu untersuchen, wann für eine Zahl

(12) $$\omega = \frac{r + s\sqrt{d}}{t}$$

die Gleichung (5), der sie genügt, nachdem man dieselbe mit dem Koeffizienten der höchsten Potenz dividiert, sie also in der Form

$$\omega^2 - 2\frac{r}{t}\omega + \frac{r^2 - ds^2}{t^2} = 0$$

geschrieben hat, ganzzahlige Koeffizienten besitzt. Hierbei darf man r, s, t ohne gemeinsamen Teiler voraussetzen, da ein solcher, wenn er vorhanden wäre, durch Heben aus (12) beseitigt werden könnte; auch kann man $t > 0$ denken, weil dies andernfalls durch Multiplikation von Zähler und Nenner mit -1 in (12) erreicht werden kann. Sollen dann

(13) $$p = \frac{2r}{t}, \quad q = \frac{r^2 - ds^2}{t^2}$$

ganze Zahlen sein, so sind zwei Fälle möglich. Entweder ist t ungerade; dann muß $\frac{r}{t}$, also der zweiten Gleichung zufolge auch $\frac{ds^2}{t^2}$ und, da d nach der Voraussetzung keinen quadratischen Teiler hat, auch $\frac{s}{t}$ eine ganze Zahl sein, r und s wären daher teilbar durch t; da aber r, s, t ohne gemeinsamen Teiler gedacht sind, müßte $t = 1$ sein. Demnach nimmt in diesem Falle die ganze Zahl (12) des Körpers die Gestalt an

(14) $$\omega = r + s\sqrt{d}$$

mit ganzzahligen Koeffizienten.

Oder t ist gerade $= 2\tau$; dann müßte $\frac{r}{\tau}$ und zufolge der zweiten der Gleichungen (13), die man in der Gestalt

$$\frac{r^2 - ds^2}{\tau^2} = 4q$$

schreiben kann, auch $\frac{ds^2}{\tau^2}$ eine ganze Zahl sein, woraus, wie zuvor, $\tau = 1$ also $t = 2$ erschlossen wird. Hiernach wäre $r^2 - ds^2 = 4q$ oder

(15) $$r^2 \equiv ds^2 \pmod{4};$$

diese Kongruenz ist aber unmöglich, wenn $d \equiv 2, 3 \pmod{4}$, es sei denn, daß r, s beide gerade genommen werden, was jedoch nicht erlaubt ist, da r, s, t ohne gemeinsamen Teiler vorausgesetzt sind. In diesem Falle haben demnach sämtliche ganze Zahlen in $\mathfrak{K}$ die Form (14). Ist dagegen $d \equiv 1 \pmod{4}$, so kann die Kongruenz (15) auch noch gelöst werden durch gleichzeitig ungerade r, s und es gibt daher in letzterem Falle außer den Zahlen von der Form (14) auch noch ganze Zahlen des Körpers von der Form

(16) $$\omega = \frac{r + s\sqrt{d}}{2},$$

worin r, s ungerade gedacht sind. Da aus der letzteren Form aber die Zahlen von der Form (14) hervorgehen, wenn r, s beide gerade gedacht werden, so kann man auch sagen: im Falle $d \equiv 1 \pmod{4}$ sind sämtliche ganze Zahlen in $\mathfrak{K}$

von der Form (16), wenn darin r, s als gleichartige Zahlen, d. h. $r \equiv s \pmod{2}$ gedacht werden.

Daß umgekehrt jede Zahl von der Form (14) resp. (16) eine ganze Zahl in $\mathfrak{K}$ vorstellt, leuchtet unmittelbar daraus ein, daß sie der Gleichung

$$\omega^2 - 2r\omega + r^2 - ds^2 = 0$$

resp.

$$\omega^2 - r\omega + \frac{r^2 - ds^2}{4} = 0$$

genügt, in deren letzter für $d \equiv 1 \pmod{4}$ und $r \equiv s \pmod{2}$ der Ausdruck $\frac{r^2 - ds^2}{4}$ einen ganzzahligen Wert hat.

Schreibt man noch in (16) $r = 2u + s$, so nimmt diese Formel die Gestalt an

(16 a) $$\omega = u + s \cdot \frac{1 + \sqrt{d}}{2},$$

worin u, s jeden ganzzahligen Wert bedeuten.

Erinnern wir uns nun des Begriffs eines Zahlenmoduls, so dürfen wir dem Ergebnisse der Untersuchung folgenden Ausdruck geben:

Die Gesamtheit aller ganzen Zahlen des quadratischen Körpers $\mathfrak{K}$, die wir stets durch das Zeichen $\mathfrak{g}$ andeuten werden, ist im Falle $d \equiv 2, 3 \pmod{4}$ identisch mit dem Zahlenmodul

(17) $$\mathfrak{g} = [1, \sqrt{d}],$$

dagegen im Falle $d \equiv 1 \pmod{4}$ identisch mit dem Zahlenmodul

(18) $$\mathfrak{g} = \left[1, \frac{1 + \sqrt{d}}{2}\right];$$

in beiden Fällen sind die Basiszahlen $1, \sqrt{d}$ bzw. $1, \frac{1 + \sqrt{d}}{2}$ selbst ganze Zahlen des Körpers.

Beide Fälle kann man folgendermaßen zusammenfassen: Sei wieder, wie bei den quadratischen Formen

(19) $$\begin{cases} D = d, & \text{wenn } d \equiv 1 \pmod{4} \\ D = 4d, & \text{wenn } d \equiv 2, 3 \pmod{4}; \end{cases}$$

dann läßt sich sowohl der Modul (17) wie (18) durch den folgenden:

(20) $$\mathfrak{g} = \left[1, \frac{D+\sqrt{D}}{2}\right]$$

ersetzen. In der Tat geht der Ausdruck

$$x + y \cdot \frac{D+\sqrt{D}}{2}$$

für $D = d$ in den anderen: $u + s \cdot \frac{1+\sqrt{d}}{2}$ über, wenn

$$x + \frac{d-1}{2} y = u, \quad y = s$$

gesetzt wird, und für $D = 4d$ in den anderen: $r + s\sqrt{d}$ durch die Substitution $x + 2dy = r$, $y = s$.

Für die Diskriminante der Zahlen $1, \frac{D+\sqrt{D}}{2}$, welche die Basis des Moduls bilden, und deren zweite auch eine ganze Zahl des Körpers ist, da sie je nach den beiden Fällen gleich $\frac{d+\sqrt{d}}{2}$ oder $2d + \sqrt{d}$, d. h. von der diesen Fällen entsprechenden Form (16) bzw. (14) ist, findet sich der Wert

$$\left(1 \cdot \frac{D-\sqrt{D}}{2} - 1 \cdot \frac{D+\sqrt{D}}{2}\right)^2 = D.$$

Diese Zahl D wird hinfort, weil für die ganze Theorie von größter Wichtigkeit, als Grundzahl des Körpers $\mathfrak{K}$ oder auch als Diskriminante des Moduls $\mathfrak{g}$, in Zeichen:

(21) $$\Delta(\mathfrak{g}) = D$$

bezeichnet werden. Auch schreiben wir zur Abkürzung

(22) $$\frac{D+\sqrt{D}}{2} = \theta$$

und daher

(23) $$\mathfrak{g} = [1, \theta].$$

4. Hieran knüpfen wir zunächst ein paar einfache Bemerkungen.

Zunächst leuchtet ein, daß jede algebraisch ganze Zahl ω des Körpers, wenn sie rational ist, sogar eine **ganze** rationale Zahl sein wird. Denn, ist sie von der Form (14), so wird, da $s = 0$ sein muß, $\omega = r$; wenn sie aber von der Form (16) ist, so wird $\omega = \frac{r}{2}$, da jedoch $r \equiv s \equiv 0 \pmod{2}$ d. i. eine gerade Zahl ist, so ist auch in diesem Falle ω einer ganzen rationalen Zahl gleich.

Ferner zeigt sich ebenso leicht, daß Summe, Differenz und Produkt zweier ganzen Zahlen ω_1, ω_2 des Körpers wieder eine solche Zahl ist. Handelt es sich um zwei Zahlen

$$\omega_1 = r_1 + s_1\sqrt{d}, \qquad \omega_2 = r_2 + s_2\sqrt{d}$$

von der Form (14), so ist dies aus den Formeln

$$\omega_1 \pm \omega_2 = (r_1 \pm r_2) + (s_1 \pm s_2)\sqrt{d}$$
$$\omega_1 \cdot \omega_2 = (r_1 r_2 + d s_1 s_2) + (r_1 s_2 + r_2 s_1)\sqrt{d}$$

offenbar. Sind aber die Zahlen

$$\omega_1 = \frac{r_1 + s_1\sqrt{d}}{2}, \qquad \omega_2 = \frac{r_2 + s_2\sqrt{d}}{2}$$

von der Form (16), in welchem Falle $d = 4\delta + 1$ gesetzt werden darf, unter δ eine ganze Zahl verstanden, so ist

$$\omega_1 \pm \omega_2 = \frac{(r_1 \pm r_2) + (s_1 \pm s_2)\sqrt{d}}{2},$$

wo $r_1 \pm r_2 \equiv s_1 \pm s_2 \pmod{2}$, weil $r_1 \equiv s_1$, $r_2 \equiv s_2 \pmod{2}$ vorauszusetzen ist; ferner ist

$$\omega_1 \cdot \omega_2 = \frac{r + s\sqrt{d}}{2},$$

wo, wenn $r_1 = s_1 + 2u_1$, $r_2 = s_2 + 2u_2$ gesetzt wird,

$$r = \frac{r_1 r_2 + d s_1 s_2}{2} = s_1 s_2 + u_1 s_2 + u_2 s_1 + 2\delta s_1 s_2 + 2u_1 u_2$$

$$s = \frac{r_1 s_2 + r_2 s_1}{2} = s_1 s_2 + u_1 s_2 + u_2 s_1,$$

also wieder $r \equiv s \pmod{2}$ ist.

Bemerken wir endlich, daß jede nicht ganze Zahl des Körpers als Quotient zweier ganzen Zahlen desselben darstellbar ist. Dies leuchtet für jede rationale Zahl des Körpers ein; jede andere Zahl ω desselben aber ist Wurzel einer quadratischen Gleichung (5), also ist $\zeta = t\omega$ Wurzel der ganzzahligen Gleichung

$$\zeta^2 - 2r\zeta + r^2 - ds^2 = 0,$$

deren höchster Koeffizient 1 ist, somit eine ganze algebraische Zahl des Körpers, und $\omega = \frac{\zeta}{t}$ ist der Quotient zweier solchen, deren Nenner t zudem, wie man sieht, als rationale ganze Zahl gedacht werden kann.

Man erkennt bis auf die verschiedene Bezeichnung in den Zahlen $r + s\sqrt{d}$ des Moduls (17) die Gitterzahlen (62 a) vorigen Kapitels, in den Zahlen $u + s \cdot \frac{1+\sqrt{d}}{2}$ des Moduls (18) die Gitterzahlen (61 a) wieder, welche den Hauptformen mit der Diskriminante $D = 4d$ resp. $D = d$ zugehörten. Die ganzen Zahlen des quadratischen Körpers mit der Grundzahl D sind also nichts anderes als diese der Hauptform mit der Diskriminante D zugehörigen Gitterzahlen. Die Norm einer solchen Zahl ω ist im ersteren Falle

$$N(\omega) = \omega \cdot \omega' = (r + s\sqrt{d})(r - s\sqrt{d}) = r^2 - ds^2,$$

im anderen Falle

$$N(\omega) = \omega \cdot \omega' = \left(u + \frac{s}{2} + \frac{s}{2}\sqrt{d}\right)\left(u + \frac{s}{2} - \frac{s}{2}\sqrt{d}\right)$$
$$= u^2 + us + \frac{1-d}{4}s^2,$$

d. i. darstellbar durch die entsprechende Hauptform. Umgekehrt ist jede durch diese Hauptform darstellbare rationale ganze Zahl m die Norm einer ganzen Zahl des quadratischen Körpers, denn aus den Gleichungen

$$m = r^2 - ds^2 \quad \text{resp.} \quad m = u^2 + us + \frac{1-d}{4}s^2$$

folgt durch Zerlegung der Form in ihre irrationalen Faktoren sogleich

$$m = \omega \cdot \omega',$$

wenn

$$\omega = r + s\sqrt{d} \quad \text{resp.} \quad \omega = u + \frac{s}{2} + \frac{s}{2}\sqrt{d} = u + s \cdot \frac{1+\sqrt{d}}{2}$$

gesetzt wird. Somit ist die Gesamtheit der durch die Hauptform darstellbaren rationalen ganzen Zahlen identisch mit der Gesamtheit der Zahlen, welche Norm einer ganzen Zahl des Körpers sein können, und es tritt auf solche Weise sogleich eine enge Zuordnung zwischen den Zahlen der Gesamtheit $\mathfrak{g}$ und der gedachten Hauptform zutage.

5. Die Gesamtheit $\mathfrak{g}$ ist aber nicht der einzige im Körper $\mathfrak{K}$ enthaltene Zahlenmodul, in welchem sich im Gegenteil unendlich viel solcher Moduln finden. Denn z. B. entspricht jeder bestimmten Zahl ω des Körpers ein in ihm enthaltener Modul $[\omega]$, d. i. die Gesamtheit aller Zahlen $x \cdot \omega$, wenn x alle rationalen ganzen Zahlen bedeutet. Desgleichen enthält $\mathfrak{K}$, wenn ω_1, ω_2 zwei voneinander unabhängige Zahlen des Körpers bezeichnen, den ganzen Modul $[\omega_1, \omega_2]$, nämlich alle Zahlen von der Form $x_1\omega_1 + x_2\omega_2$ für ganzzahlige x_1, x_2. Ein Modul der letzteren Art soll zum Unterschiede von denen der ersteren ein **zweigliedriger Modul** und ω_1, ω_2 seine **Basis** heißen; diese Basis ist stets auch zugleich eine Basis des Körpers. Sind insbesondere ω_1, ω_2 **ganze** Zahlen des Körpers, d. h. Zahlen in $\mathfrak{g}$, so sind nach der zweiten Bemerkung voriger Nummer auch alle Zahlen des Moduls $[\omega_1, \omega_2]$ solche Zahlen, der gesamte Modul also nur ein Teil des Moduls $\mathfrak{g}$.

Da auf die Eigenschaften derartiger Moduln die ganze Theorie des Körpers $\mathfrak{K}$ sich begründet, müssen wir die wesentlichsten derselben gleich im voraus besprechen. Sei

$$\mathfrak{m} = [\omega_1, \omega_2] \tag{24}$$

ein zweigliedriger Modul ganzer Zahlen des Körpers und ξ_1, ξ_2 irgend zwei in ihm enthaltene Zahlen, so bestehen zwei Gleichungen

$$\xi_1 = a\omega_1 + b\omega_2, \quad \xi_2 = c\omega_1 + d\omega_2 \tag{25}$$

mit ganzzahligen Koeffizienten a, b, c, d. Daraus folgt

$$(ad - bc)\cdot\omega_1 = d\xi_1 - b\xi_2, \quad (ad - bc)\cdot\omega_2 = -c\xi_1 + a\xi_2. \tag{26}$$

Demnach sind, wenn

$$ad - bc = \pm 1 \tag{27}$$

ist, auch umgekehrt ω_1, ω_2 und folglich auch alle Zahlen $\omega = x_1 \omega_1 + x_2 \omega_2$ des Moduls $\mathfrak{m}$ linear durch ξ_1, ξ_2 mit ganzzahligen Koeffizienten darstellbar, d. h. Zahlen des Moduls $[\xi_1, \xi_2]$, und da auch jede Zahl des letzteren zugleich mit ξ_1, ξ_2 in $\mathfrak{m}$ enthalten sein muß, so ergibt sich die Gleichheit der Moduln $[\omega_1, \omega_2]$ und $[\xi_1, \xi_2]$ (vgl. Kap. 4, Nr. 1). — Die hierfür ausreichende Bedingung (27) ist zudem aber auch dafür notwendig; denn, sollen diese Moduln identisch sein, so muß der Ausdruck $x_1 \omega_1 + x_2 \omega_2$ für jedes ganzzahlige Wertsystem x_1, x_2 dem Ausdrucke $y_1 \xi_1 + y_2 \xi_2$, d. i. dem Ausdrucke

$$(a y_1 + c y_2) \cdot \omega_1 + (b y_1 + d y_2) \cdot \omega_2$$

für ein entsprechendes ganzzahliges Wertsystem y_1, y_2 gleich sein, und umgekehrt, d. h. die Gleichungen

$$x_1 = a y_1 + c y_2, \qquad x_2 = b y_1 + d y_2$$

müssen für ganzzahlige x_1, x_2 auch ganzzahlige y_1, y_2 ergeben, und umgekehrt, was nach Kap. 4, Nr. 1 des vorigen Abschnitts nur dann geschieht, wenn $ad - bc = \pm 1$ ist. Wir haben also folgenden

Satz: Zwei zweigliedrige Moduln in $\mathfrak{g}$:

$$[\xi_1, \xi_2], \qquad [\omega_1, \omega_2]$$

sind dann und nur dann miteinander identisch, wenn zwischen ihren Basen Gleichungen bestehen von der Form (25), in denen a, b, c, d ganze rationale, der Bedingung (27) genügende Zahlen bezeichnen.

Oder auch: Aus einer Basis ω_1, ω_2 des zweigliedrigen Moduls $\mathfrak{m}$ erhält man jede andere Basis desselben vermittels der Gleichungen (25), wenn darin für a, b, c, d sämtliche der Bedingung (27) genügende ganze Zahlen gesetzt werden.

Denkt man in die Gleichungen (25) die Werte von $\xi_1, \xi_2, \omega_1, \omega_2$ eingesetzt, so müssen sie bestehen bleiben, wenn das Vorzeichen der in den letzteren auftretenden Irrationalität $\sqrt{d}$ verändert wird; mit anderen Worten: zwischen den zu jenen Zahlen konjugierten Zahlen $\xi_1', \xi_2', \omega_1', \omega_2'$ bestehen die völlig entsprechenden Gleichungen

$$(25') \qquad \xi_1' = a \omega_1' + b \omega_2', \qquad \xi_2' = c \omega_1' + d \omega_2'.$$

Daraus aber erschließt man nach einfacher Berechnung die Beziehung

$$\xi_1 \xi_2' - \xi_2 \xi_1' = (a d - b c) \cdot (\omega_1 \omega_2' - \omega_2 \omega_1'),$$

aus welcher unter Voraussetzung der Gleichung (27) diese andere

$$\xi_1 \xi_2' - \xi_2 \xi_1' = \pm(\omega_1 \omega_2' - \omega_2 \omega_1')$$

und folglich durch Quadrierung die Gleichung

$$\Delta(\xi_1, \xi_2) = \Delta(\omega_1, \omega_2)$$

hervorgeht. Die Diskriminante der Basis eines zweigliedrigen Moduls $\mathfrak{m}$ in $\mathfrak{g}$ ist somit eine von der besonderen Wahl dieser Basis unabhängige, nur durch den Modul selbst bestimmte Zahl und soll deshalb die Diskriminante des Moduls genannt und kurz mit $\Delta(\mathfrak{m})$ bezeichnet werden. Sie ist stets eine ganze rationale Zahl; denn einerseits ist sie (nach Nr. 2) rational, andererseits als eine aus den ganzen algebraischen Zahlen $\omega_1, \omega_2, \omega_1', \omega_2'$ nur durch Addition oder Subtraktion und Multiplikation gebildete Zahl (nach Nr. 4) eine ganze algebraische, daher auch eine ganze rationale Zahl.

6. Der Modul $\mathfrak{g} = [1, \theta]$ aller ganzen Zahlen des Körpers ist ein zweigliedriger Modul mit der Basis $1, \theta$, dessen sämtliche anderen Basen γ_1, γ_2 dem Vorigen zufolge durch die Formeln

$$(28) \qquad \gamma_1 = \alpha + \beta\theta, \quad \gamma_2 = \gamma + \delta\theta$$

erhalten werden, wenn $\alpha, \beta, \gamma, \delta$ ganze Zahlen sind, welche der Bedingung $\alpha\beta - \gamma\delta = \pm 1$ Genüge leisten; man kann daher dann auch schreiben

$$(29) \qquad \mathfrak{g} = [\gamma_1, \gamma_2].$$

Für die Diskriminante

$$\Delta(\gamma_1, \gamma_2) = \Delta(1, \theta) = (\theta' - \theta)^2$$

fanden wir bereits in (21) den Wert

$$(30) \qquad \Delta(\mathfrak{g}) = D,$$

d. i. gleich der Grundzahl des Körpers.

Es soll nun gezeigt werden, daß auch jeder in $\mathfrak{g}$ enthaltene Modul $\mathfrak{m}$, welcher zwei unabhängige Zahlen ω_1, ω_2 enthält, ein zweigliedriger Modul ist. Die Zahlen ω_1, ω_2

können als unabhängige ganze Zahlen des Körpers in der Form

$$\omega_1 = a\gamma_1 + b\gamma_2, \quad \omega_2 = c\gamma_1 + d\gamma_2$$

geschrieben werden, worin a, b, c, d ganze Zahlen sind, für welche der Ausdruck $\Delta = ad - bc$ nicht verschwindet (Nr. 2). Hierbei darf Δ positiv gedacht werden, da andernfalls dies erreicht würde, wenn man ω_2 durch $-\omega_2$ ersetzte, d. h. c, d mit entgegengesetztem Vorzeichen nähme, was erlaubt ist, da $\omega_1, -\omega_2$ ebensogut wie ω_1, ω_2 unabhängige Zahlen sind. Daraus folgt

$$\Delta\gamma_1 = d\omega_1 - b\omega_2, \quad \Delta\gamma_2 = -c\omega_1 + a\omega_2;$$

$\Delta\gamma_1, \Delta\gamma_2$ sind also zugleich mit ω_1, ω_2 Zahlen des Moduls $\mathfrak{m}$. Nun sind alle Zahlen dieses Moduls als ganze Zahlen des Körpers von der Form

$$z_1\gamma_1 + z_2\gamma_2$$

und unter ihnen gibt es solche, bei denen z_2 positiv ist, z. B. die Zahl $\Delta\gamma_2$, also auch solche, bei denen z_2 einen kleinsten positiven Wert hat; eine solche Zahl sei

$$\xi_2 = l\gamma_1 + n\gamma_2.$$

Ferner gibt es in $\mathfrak{m}$ auch Zahlen von der Form $z_1\gamma_1$ mit positivem z_1, z. B. die Zahl $\Delta\gamma_1$; sei

$$\xi_1 = m\gamma_1$$

diejenige von ihnen, wo z_1 den kleinsten positiven Wert m hat. Es wird behauptet, daß diese Zahlen

$$\xi_1 = m\gamma_1, \quad \xi_2 = l\gamma_1 + n\gamma_2, \tag{31}$$

welche unabhäng sind, da die Determinante der Gleichungen gleich $m \cdot n$, also von Null verschieden ist, eine Basis von $\mathfrak{m}$ bilden. Setzt man nämlich in der Zahl

$$\omega = z_1\gamma_1 + z_2\gamma_2$$

dieses Moduls

$$z_2 = q_2 n + r_2, \quad z_1 - q_2 l = q_1 m + r_1,$$

worin

$$0 \gtreqless r_1 < m, \quad 0 \gtreqless r_2 < n \tag{32}$$

gedacht wird, so findet sich

$$\omega = r_1\gamma_1 + r_2\gamma_2 + q_1\xi_1 + q_2\xi_2;$$

da nun ω, ξ_1, ξ_2 Zahlen in $\mathfrak{m}$ sind, so ist auch $r_1 \gamma_1 + r_2 \gamma_2$ eine solche Zahl, wegen $r_2 < n$ und nach der Bedeutung von n ergibt sich deshalb $r_2 = 0$, und da dann die Zahl gleich $r_1 \gamma_1$ wird, muß wegen $r_1 < m$ und nach der Bedeutung von m auch $r_1 = 0$ sein. Demnach hat jede Zahl ω des Moduls $\mathfrak{m}$ die Form

$$\omega = q_1 \xi_1 + q_2 \xi_2 ,$$

d. h. sie ist enthalten im Modul $[\xi_1, \xi_2]$, und da umgekehrt jede Zahl des letzteren zugleich mit ξ_1, ξ_2 eine Zahl des Moduls $\mathfrak{m}$ ist, sind beide Moduln identisch:

$$\mathfrak{m} = [\xi_1, \xi_2] ,$$

d. h. die beiden unabhängigen Zahlen ξ_1, ξ_2 sind eine Basis von $\mathfrak{m}$ und somit $\mathfrak{m}$ ein zweigliedriger Modul, w. z. b. w.

Für irgend eine andere Basis ζ_1, ζ_2 desselben Moduls bestehen Gleichungen von der Form

$$\zeta_1 = a \xi_1 + b \xi_2 , \quad \zeta_2 = c \xi_1 + d \xi_2$$

mit der Bedingung $ad - bc = \pm 1$; durch Substitution der Werte (31) für ξ_1, ξ_2 gehen sie über in die folgenden:

$$\zeta_1 = (am + bl)\gamma_1 + bn\gamma_2 , \quad \zeta_2 = (cm + dl)\gamma_1 + dn\gamma_2 .$$

Schreibt man dafür einfacher

$$(33) \qquad \zeta_1 = \alpha\gamma_1 + \beta\gamma_2 , \quad \zeta_2 = \gamma\gamma_1 + \delta\gamma_2 ,$$

so findet man die Beziehung

$$(34) \qquad \alpha\delta - \beta\gamma = (ad - bc) \cdot mn = \pm mn .$$

7. Sei jetzt

$$\omega = z_1 \gamma_1 + z_2 \gamma_2$$

irgend eine Zahl in $\mathfrak{g}$; man erhält dann wieder

$$\omega = r_1 \gamma_1 + r_2 \gamma_2 + q_1 \xi_1 + q_2 \xi_2$$

und folglich ist die Differenz $\omega - (r_1 \gamma_1 + r_2 \gamma_2)$ eine Zahl des Moduls $\mathfrak{m}$. Nun führen wir eine wichtige Verallgemeinerung des Kongruenzbegriffes ein. Erinnern wir uns, daß zwei rationale ganze Zahlen a, b kongruent genannt wurden (mod. m), wenn ihre Differenz durch m teilbar oder eine Zahl des Moduls $[m]$ war. In gleicher

Weise sollen fortan zwei ganze Zahlen ω_1, ω_2 des Körpers $\mathfrak{K}$ kongruent heißen in bezug auf einen Modul $\mathfrak{m}$, in Zeichen:

$$\omega_1 \equiv \omega_2 \pmod{\mathfrak{m}},$$

wenn ihre Differenz eine Zahl dieses Moduls ist.

Hiernach dürfen wir unser Ergebnis dahin aussprechen, daß wir sagen:

Jede ganze Zahl des Körpers ist in bezug auf den Modul $\mathfrak{m}$ der vorigen Nummer einer Zahl $r_1\gamma_1 + r_2\gamma_2$ kongruent, in welcher r_1, r_2 durch die Ungleichheiten (31) beschränkt sind. Es leuchtet aber wieder ein, daß zwei ganze Zahlen, welche derselben dritten ganzen Zahl kongruent sind, es auch untereinander sein werden; man kann also auch hier alle ganzen Zahlen des Körpers in Klassen (mod. $\mathfrak{m}$) kongruenter Zahlen verteilen, indem man alle mit derselben Zahl $r_1\gamma_1 + r_2\gamma_2$ (mod. $\mathfrak{m}$) kongruenten Zahlen in eine Klasse vereinigt; daher wird die Anzahl dieser Klassen so groß sein, wie die Anzahl der nicht kongruenten Zahlen dieser Art. Nun können aber zwei nicht identische Zahlen dieser Art:

$$(35) \qquad r_1'\gamma_1 + r_2'\gamma_2, \quad r_1''\gamma_1 + r_2''\gamma_2$$

einander nicht kongruent sein, denn wäre etwa $r_2' \geqq r_2''$, so müßte dann die Differenz

$$(r_1' - r_1'')\gamma_1 + (r_2' - r_2'')\gamma_2$$

dem Modul $\mathfrak{m}$ angehören, was, da $r_2' - r_2''$ eine nicht negative Zahl $< n$ wäre, nur sein kann, wenn $r_2' = r_2''$, die Differenz also gleich $(r_1' - r_1'')\gamma_1$ wäre, diese aber könnte wieder nur dann dem Modul $\mathfrak{m}$ angehören, wenn es auch die entgegengesetzte Zahl $(r_1'' - r_1')\gamma_1$ täte, und da in einer von beiden der Koeffizient von γ_1 nicht negativ und $< m$ wäre, müßte auch $r_1' = r_1''$, die Zahlen (35) also identisch sein.

Aus diesem Umstande ist zu schließen, daß die Anzahl von Klassen (mod. $\mathfrak{m}$) kongruenter Zahlen, in welche sich die Zahlen der Gesamtheit $\mathfrak{g}$ verteilen, genau so groß ist, wie die Anzahl der Zahlen $r_1\gamma_1 + r_2\gamma_2$, d. h. so groß, wie die Anzahl der Kombinationen aus den zulässigen Werten von r_1 und r_2, also zufolge der Ungleichheiten (32) gleich $m \cdot n$. Wir nennen diese Anzahl von Klassen die Norm des Moduls $\mathfrak{m}$ und bezeichnen sie mit $\mathfrak{N}(\mathfrak{m})$. Die Zahlen $r_1\gamma_1 + r_2\gamma_2$ dürfen als Repräsentanten der Klassen

angesehen oder auch als ein vollständiges Restsystem der ganzen Zahlen des Körpers (mod. $\mathfrak{m}$) bezeichnet werden. Ist insbesondere $\mathfrak{m} = \mathfrak{g}$, so ergibt sich der Definition der Norm zufolge offenbar

$$\mathfrak{N}(\mathfrak{g}) = 1.$$

Beachtet man die Gleichung (34) voriger Nummer, so kann man das erhaltene Resultat auch in folgenden **Satz** fassen:

Ist $\mathfrak{m} = [\zeta_1, \zeta_2]$ ein zweigliedriger Modul ganzer Zahlen des Körpers und sind seine Basiszahlen durch die Basiszahlen γ_1, γ_2 des Moduls $\mathfrak{g}$ mittels der Formeln (33) bestimmt, so ist die Anzahl der Klassen (mod. $\mathfrak{m}$) kongruenter Zahlen, in welche sich die sämtlichen ganzen Zahlen des Körpers verteilen, oder die Anzahl der Glieder eines vollständigen Restsystems (mod. $\mathfrak{m}$)

(36) $$\mathfrak{N}(\mathfrak{m}) = \pm(\alpha\delta - \beta\gamma).$$

Aus den Formeln (33) findet man ferner

$$\zeta_1 \zeta_2' - \zeta_2 \zeta_1' = (\alpha\delta - \beta\gamma) \cdot (\gamma_1 \gamma_2' - \gamma_2 \gamma_1'),$$

mithin durch Quadrierung

$$\Delta(\zeta_1, \zeta_2) = (\alpha\delta - \beta\gamma)^2 \cdot \Delta(\gamma_1, \gamma_2)$$

oder

$$\Delta(\mathfrak{m}) = (\alpha\delta - \beta\gamma)^2 \cdot \Delta(\mathfrak{g}).$$

Mit Rücksicht auf (30) und (36) liefert diese Formel die wichtige Beziehung:

(37) $$\Delta(\mathfrak{m}) = \mathfrak{N}(\mathfrak{m})^2 \cdot D.$$

8. Haben wir im Vorigen die Basis γ_1, γ_2 von $\mathfrak{g}$ beliebig gedacht, so wollen wir nunmehr im besonderen die Basis $1, \theta$ dafür wählen. Dann erhält nach (31) der Modul $\mathfrak{m}$ eine Basis $\xi_1 = m$, $\xi_2 = l + n\theta$, so daß

$$\mathfrak{m} = [m, l + n\theta]$$

gesetzt werden kann. Führen wir nun die Zahl

$$\omega = \frac{l + n\theta}{m}$$

ein, so läßt sich noch einfacher schreiben

(38) $$\mathfrak{m} = m[1, \omega]$$

Da nun ω eine irrationale Zahl des Körpers $\mathfrak{K}$ bedeutet, ist sie Wurzel einer quadratischen Gleichung

$$(39) \qquad a z^2 + b z + c = 0$$

mit ganzzahligen Koeffizienten, deren erster positiv und welche zusammen ohne gemeinsamen Teiler gedacht werden dürfen. Somit bestehen die Beziehungen

$$(40) \qquad \begin{cases} a\omega^2 + b\omega + c = 0 \\ \omega + \omega' = \dfrac{-b}{a}, \quad \omega \cdot \omega' = \dfrac{c}{a} \\ \omega = \dfrac{-b \pm \sqrt{\Delta}}{2a}, \end{cases}$$

wenn

$$(41) \qquad b^2 - 4ac = \Delta$$

gesetzt wird. Hiernach ist

$$(a\omega)^2 + b \cdot (a\omega) + ac = 0\,,$$

mithin $a\omega$ eine ganze algebraische Zahl des Körpers, so daß mit ganzzahligen h, k

$$(42) \qquad a\omega = h + k\theta$$

gesetzt und dabei k positiv angenommen werden kann, da man andernfalls dies erreichen würde, wenn man, was erlaubt ist, da

$$x + \omega y = x - \omega(-y)$$

gesetzt werden kann, also $[1, \omega] = [1, -\omega]$ ist, im Modul (38) die Basiszahl ω durch $-\omega$ ersetzte. Die Vergleichung von (42) mit der dritten der Formeln (40) ergibt dann mit Rücksicht auf den Wert $\theta = \dfrac{D + \sqrt{D}}{2}$ die Beziehung

$$(43) \qquad \Delta = k^2 \cdot D\,.$$

Nun ist mit dem Modul $\mathfrak{m}$ ein anderer Modul $\mathfrak{o}$ enge verbunden, den wir die Ordnung von $\mathfrak{m}$ nennen wollen. Suchen wir die Gesamtheit $\mathfrak{o}$ aller Zahlen α von der Eigenschaft, daß jedes Produkt $\alpha\gamma$ aus α und einer Zahl γ des Moduls $\mathfrak{m}$ wieder diesem Modul angehöre. Solche Zahlen gibt es, da z. B. für jede rationale ganze Zahl r der De-

finition eines Zahlenmoduls entsprechend zugleich mit γ auch das Produkt $r \cdot \gamma$ in $\mathfrak{m}$ enthalten ist; auch leuchtet ein, daß sie einen Modul bilden, denn, sind α, α' zwei solche Zahlen, daß jedes der Produkte $\alpha\gamma, \alpha'\gamma$ in $\mathfrak{m}$ enthalten ist, so sind es auch $(\alpha \pm \alpha')\gamma$, d. h. mit α, α' zugleich gehören auch $\alpha \pm \alpha'$ der Gesamtheit $\mathfrak{o}$ an. Offenbar sind nun die gesuchten Zahlen α dieselben wie diejenigen, für welche jedes Produkt $\alpha\gamma$ aus α und einer Zahl γ des einfacheren Moduls $[1, \omega]$ diesem letzteren Modul angehört. Soll α eine solche Zahl sein, so müssen vor allem die Produkte $\alpha \cdot 1$ und $\alpha \cdot \omega$ dem Modul $[1, \omega]$ angehören, mithin erstlich $\alpha = x + y\omega$ sein, während x, y ganze rationale Zahlen bezeichnen; zweitens ist dann

$$\alpha\omega = x\omega + y\omega^2 = \left(x - \frac{by}{a}\right)\omega - \frac{cy}{a},$$

damit also auch $\alpha\omega$ eine Zahl jenes Moduls sei, müssen $\frac{by}{a}, \frac{cy}{a}$ ganze Zahlen, also by, cy durch a teilbar sein, was y durch a teilbar erfordert, da a, b, c ohne gemeinsamen Teiler sind. Setzt man demgemäß $y = az$, so muß jede Zahl α der gedachten Art die Form

$$(44) \qquad \alpha = x + z \cdot a\omega$$

haben. Aber jede Zahl dieser Form ist auch wirklich eine der gesuchten, denn, bedeutet $\gamma = u + v\omega$ irgend eine Zahl des Moduls $[1, \omega]$, so findet sich

$$\begin{aligned}\alpha\gamma &= (x + z \cdot a\omega) \cdot (u + v\omega) = xu + (zua + xv)\omega + zav\omega^2 \\ &= (xu - czv) + (azu + xv - bzv) \cdot \omega,\end{aligned}$$

d. h. $\alpha\gamma$ ist eine Zahl in $[1, \omega]$. Die Gesamtheit $\mathfrak{o}$ ist also die Gesamtheit aller Zahlen von der Form (44), d. h. der Modul

$$(45) \qquad \mathfrak{o} = [1, a\omega].$$

Schreibt man aber (44) mit Beachtung von (42) in der Form

$$\alpha = (x + hz) + kz\theta$$

und bedenkt, daß $x + hz, z$ ebensogut wie x, z selbst jedes Paar ganzer Zahlen ausmachen, so darf man die Ordnung von $\mathfrak{m}$ auch durch folgende Gleichung definieren:

$$(46) \qquad \mathfrak{o} = [1, k\theta].$$

Hieraus folgen noch die Gleichungen

(47) $$\Delta(\mathfrak{o}) = k^2 \cdot \Delta(\mathfrak{g}) = k^2 \cdot D\,,$$

mithin

(48) $$\Delta = \Delta(\mathfrak{o})\,, \qquad k = \mathfrak{N}(\mathfrak{o})\,.$$

Aus diesen Beziehungen ist zu entnehmen, daß jede Ordnung eines zweigliedrigen Moduls $\mathfrak{m}$ ganzer Zahlen des Körpers ebenfalls ein solcher Modul ist, welcher zudem mit der Einheit zugleich alle rationalen ganzen Zahlen enthält. Diese Eigenschaft ist, wie man leicht erkennt, für die Ordnungen eines quadratischen Körpers*) charakteristisch. In der Tat ist jeder Modul desselben von der angegebenen Beschaffenheit die Ordnung eines Moduls, nämlich jedenfalls seine eigene. Denn, setzt man ihn in die allgemeine Form $m \cdot [1, \omega]$, so muß m als die offenbar kleinste in ihm enthaltene positive ganze Zahl gleich 1, der Modul also von der Form $[1, \omega]$ und daher ω eine ganze Zahl des Körpers, d. i. Wurzel einer ganzzahligen Gleichung

$$\omega^2 + b\,\omega + c = 0$$

sein, aus welcher $\omega^2 = -b\,\omega - c$ als im Modul enthalten hervorgeht. Deshalb wird jede Zahl von der Form $x + y\,\omega$, die, wie oben gezeigt, für die Zahlen der Ordnung unseres Moduls $[1, \omega]$ notwendig ist, auch wirklich seiner Ordnung angehören, da das Produkt

$$(x + y\,\omega) \cdot (u + v\,\omega)$$

wieder in die Gestalt $u' + v'\omega$ gebracht werden kann, also dem Modul $[1, \omega]$ angehört. Somit findet sich in der Tat die Ordnung unseres Moduls mit ihm selber identisch, d. h. der gedachte Modul ist eine Ordnung, w. z. b. w.

Hieraus folgt insbesondere, daß die Gesamtheit $\mathfrak{g}$ aller ganzen Zahlen des Körpers eine Ordnung ist.

9. Nunmehr beschränken wir die fernere Betrachtung auf eine Kategorie von Moduln ganzer Zahlen des Körpers $\mathfrak{K}$, welche durch die Eigenschaft ausgezeichnet sind, daß ihre Ordnung $\mathfrak{o}$ identisch ist mit $\mathfrak{g}$. Daß es solche Moduln gibt, leuchtet von vornherein daraus ein, daß $\mathfrak{g}$ selbst einer

*) Statt des Ausdrucks „Ordnung" wird auch die Bezeichnung „Zahlenring" verwendet.

ist. Jeder Modul dieser Art soll nach dem Vorgange von *Dedekind* ein Ideal heißen, für welches also folgende **Definition** aufgestellt werden kann:

Ein Ideal des Körpers $\mathfrak{K}$ ist ein Modul ganzer Zahlen desselben von der ausgezeichneten Eigenschaft, daß alle seine Zahlen mit irgend einer ganzen Zahl multipliziert wieder Zahlen des Moduls sind.

Daß jedes Ideal ein zweigliedriger Modul ist, also unter die voraufgehenden Betrachtungen fällt, geht daraus hervor, daß, wenn ζ irgend eine in ihm enthaltene Zahl bezeichnet, auch $\zeta \cdot \theta$ ihm angehören muß, diese beiden Zahlen aber ebenso wie 1 und θ unabhängige Zahlen sind.

Da für ein Ideal die Ordnung $\mathfrak{o}$ gleich $\mathfrak{g}$ ist, folgt mit Beachtung von (46) dann $k = 1$, also aus (43) $\varDelta = D$. Demnach hat jedes Ideal j die Form

$$j = [m, m\,\omega],$$

während nach (45) seine Ordnung $\mathfrak{g}$ auch als der Modul $[1, a\,\omega]$ bezeichnet werden darf; da nun $m\,\omega$ eine ganze Zahl, d. i. eine Zahl des letzteren Moduls ist, darf man $m\,\omega = r + s \cdot a\,\omega$, d. h. $r = 0$, $m = a\,s$ und

(49) $$j = s\,a \cdot [1, \omega)$$

setzen, worin nach (40) und (42)

$$a\,\omega = h + \theta = \frac{-b + \sqrt{D}}{2}$$

ist, während a eine positive und b eine ganze Zahl bezeichnet, für welche

(50) $$b^2 \equiv D \pmod{4\,a}$$

oder $b^2 - 4\,a\,c = D$ ist. Diese für ein Ideal notwendige Form (49) ist aber dazu auch ausreichend und somit ist sie für die Ideale charakteristisch. In der Tat genügt es zu zeigen, daß dann auch die Zahlen $s\,a \cdot \theta$ und $s\,a\,\omega \cdot \theta$ dem Modul angehören, denn alsdann sind auch alle Produkte

$$(u + v\theta) \cdot (s\,a\,x + s\,a\,\omega\,y)$$
$$= u\,x \cdot s\,a + u\,y \cdot s\,a\,\omega + v\,x \cdot s\,a\,\theta + v\,y \cdot s\,a\,\omega\,\theta$$

aus irgend einer Zahl in $\mathfrak{g}$ mit irgend einer Zahl des Moduls in diesem enthalten. Dies folgt aber unmittelbar aus nachstehenden Gleichungen:

$$a\theta = \frac{D+b}{2}\cdot a + a\cdot\frac{-b+\sqrt{D}}{2} = \frac{D+b}{2}\cdot a + a\cdot a\omega\,,$$

$$a\omega\theta = \frac{D-b^2}{4} + \frac{-b+D}{2}\cdot\frac{-b+\sqrt{D}}{2} = -c\cdot a + \frac{-b+D}{2}\cdot a\omega\,,$$

wenn man bemerkt, daß in diesen $\frac{b+D}{2}$ und $\frac{-b+D}{2}$ ganze Zahlen sind, da aus (50) sich $b \equiv D \pmod{2}$, d. i. b, D sich als gleichartige Zahlen ergeben.

Aus den Beziehungen

$$sa = sa\cdot 1 + 0\cdot\theta\,,\qquad sa\omega = sh\cdot 1 + s\cdot\theta$$

folgen nach (36) und (37) die Formeln

$$\mathfrak{N}(j) = s^2 a\,,\qquad \Delta(j) = s^4 a^2\cdot D\,. \tag{51}$$

10. Für das besondere Ideal $\mathfrak{g}$ ist in Nr. 4 ein inniger Zusammenhang mit der Hauptform von der Diskriminante D festgestellt, insofern alle durch die letztere darstellbaren ganzen rationalen Zahlen Normen von Zahlen in $\mathfrak{g}$ sind, und umgekehrt. Für ein beliebiges Ideal j läßt sich ganz ähnliches nachweisen. In der Tat, ist

$$\zeta = sa\cdot x - \frac{-b+\sqrt{D}}{2}\cdot sy \tag{52}$$

irgend eine in j enthaltene Zahl, so findet sich

$$\left\{\begin{aligned} N(\zeta) &= s^2\left(\left(ax+\frac{b}{2}y\right)^2 - D\cdot\frac{y^2}{4}\right)\\ &= s^2a\cdot(ax^2+bxy+cy^2) = \mathfrak{N}(j)\cdot(ax^2+bxy+cy^2)\,, \end{aligned}\right. \tag{53}$$

d. h. die Norm jeder in j enthaltenen Zahl ist das Produkt aus der Norm des Ideals in eine durch die Form (a, b, c) mit der Diskriminante D und positivem ersten Koeffizienten darstellbare Zahl

$$m = ax^2 + bxy + cy^2\,.$$

Umgekehrt, wenn letztere Gleichung besteht, so ist durch Zerlegung der Form in ihre irrationalen Faktoren rückwärts zu schließen, daß die durch (52) definierte Zahl ζ eine Zahl des Ideals j ist, deren Norm gleich $\mathfrak{N}(j)\cdot m$ ist. Dies Resultat ist nur eine Verallgemeinerung des in Nr. 4 für $\mathfrak{g}$

erhaltenen, denn wenn $j = \mathfrak{g}$ gesetzt wird, ist gleichzeitig $\mathfrak{N}(j) = \mathfrak{N}(\mathfrak{g}) = 1$ zu setzen.

So findet sich also jedem Ideale j eine bestimmte quadratische Form (a, b, c) mit der Diskriminante D und positivem ersten Koeffizienten aufs engste zugeordnet. Da die Koeffizienten dieser Form nur durch a und $a\omega$ bestimmt, aber von s unabhängig sind, so entspricht dieselbe Form unendlich viel Idealen, deren eines $j = [a, a\omega]$ ist, während die andern hieraus durch Multiplikation mit einer beliebigen ganzen Zahl s hervorgehen. — Aber auch umgekehrt ist jeder Form (a, b, c) mit der Diskriminante D und positivem ersten Koeffizienten eine solche Serie von Idealen des Körpers mit der Grundzahl D zugeordnet. Denn ist $\omega = \frac{-b+\sqrt{D}}{2a}$ die erste Wurzel der quadratischen Form, so ist $s \cdot [a, a\omega]$ für jedes ganzzahlige s nach voriger Nummer ein Ideal j, das mit der Form (a, b, c) in dem zuvor erwähnten Zusammenhange steht.

Nun sei aber $a_1 x_1^2 + b_1 x_1 y_1 + c_1 y_1^2$ eine zweite Form mit der Diskriminante D und positivem ersten Koeffizienten, von der wir annehmen wollen, sie sei eigentlich äquivalent mit der Form $ax^2 + bxy + cy^2$, so daß diese durch eine Substitution

$$x = \alpha x_1 + \beta y_1, \quad y = \gamma x_1 + \delta y_1$$

in jene und umgekehrt die letztere durch die Substitution

$$x_1 = \delta x - \beta y, \quad y_1 = -\gamma x + \alpha y$$

in die erstere übergeht, während $\alpha\delta - \beta\gamma = 1$ sei. Dann wird

$$a_1 \delta^2 - b_1 \delta \gamma + c_1 \gamma^2 = a \tag{54}$$

sein und zwischen den ersten Wurzeln ω, ω_1 beider Formen diese Gleichung bestehen:

$$\omega = \frac{\alpha\omega_1 + \beta}{\gamma\omega_1 + \delta}. \tag{55}$$

Dem Voraufgehenden zufolge ist der Form (a, b, c) ein Ideal $j = [a, a\omega]$, der Form (a_1, b_1, c_1) ein Ideal $j_1 = [a_1, a_1\omega_1]$ des Körpers $\mathfrak{K}$ zugeordnet. Dem ersten von beiden kann man die Form geben:

$$j = \frac{a}{a_1} \cdot [a_1, a_1\omega] = \frac{a}{\delta a_1 + \gamma a_1 \omega_1} \cdot [\delta a_1 + \gamma a_1 \omega_1, \beta a_1 + \alpha a_1 \omega_1].$$

Hier ist der Modul zur Rechten gleich dem Ideale j_1, denn seine Basiszahlen sind lineare Verbindungen der Basiszahlen $a_1, a_1\omega_1$ von j_1, während die Koeffizienten der Verbindung die Gleichung $\delta \cdot \alpha - \gamma \cdot \beta = 1$ erfüllen. Andererseits ist der Nenner $\delta a_1 + \gamma a_1 \omega_1$ eine ganze Zahl des Körpers $\mathfrak{K}$, deren Norm $(\delta a_1 + \gamma a_1 \omega_1) \cdot (\delta a_1 + \gamma a_1 \omega_1')$ wegen $\omega_1 + \omega_1' = \frac{-b_1}{a_1}$, $\omega_1 \omega_1' = \frac{c_1}{a_1}$ sich leicht gleich

$$a_1 (a_1 \delta^2 - b_1 \delta \gamma + c_1 \gamma^2) = a_1 a$$

findet; der Bruch $\frac{a}{\delta a_1 + \gamma a_1 \omega_1}$ ist demnach eine Zahl η des Körpers, deren Norm gleich $\frac{a^2}{a_1 a} = \frac{a}{a_1}$, mithin positiv ist. Aus der angenommenen eigentlichen Äquivalenz der Formen (a, b, c), (a_1, b_1, c_1) folgt also die Existenz einer Zahl η des Körpers mit positiver Norm von der Beschaffenheit, daß zwischen den den Formen zugeordneten Idealen j, j_1 die Beziehung

$$j = \eta \cdot j_1 \tag{56}$$

besteht.

Umgekehrt, wenn eine solche Beziehung zwischen zwei Idealen stattfindet, so sind die beiden ihnen zugeordneten quadratischen Formen einander eigentlich äquivalent. Denn aus

$$[a, a\omega] = \eta \cdot [a_1, a_1 \omega_1] = [\eta a_1, \eta a_1 \omega_1]$$

folgt zunächst, daß $\eta a_1, \eta a_1 \omega_1$, also auch ihre Konjugierten ganze Zahlen des Körpers sein müssen, ferner aber, daß zwischen den Basen der beiden Moduln bzw. ihren Konjugierten Gleichungen bestehen müssen von der Form

$$(57)\begin{cases} a = \alpha \cdot \eta a_1 + \beta \cdot \eta a_1 \omega_1, & a\omega = \gamma \cdot \eta a_1 + \delta \cdot \eta a_1 \omega_1, \\ a = \alpha \cdot \eta' a_1 + \beta \cdot \eta' a_1 \omega_1', & a\omega' = \gamma \cdot \eta' a_1 + \delta \cdot \eta' a_1 \omega_1', \end{cases}$$

worin $\alpha, \beta, \gamma, \delta$ rationale ganze, der Bedingung $\alpha\delta - \beta\gamma = \pm 1$ genügende Zahlen sind, Gleichungen, aus denen die folgende:

$$\omega = \frac{\gamma + \delta \omega_1}{\alpha + \beta \omega_1},$$

d. i. die Äquivalenz der Zahlen ω, ω_1, also auch diejenige der Formen (a, b, c), (a_1, b_1, c_1), deren erste Wurzeln sie

sind, erschlossen wird. Diese Äquivalenz ist zudem die eigentliche, denn aus (57) leitet man die Gleichung

$$a \cdot a\omega' - a\omega \cdot a = (\alpha\delta - \beta\gamma) \cdot (\eta a_1 \cdot \eta' a_1 \omega_1' - \eta a_1 \omega_1 \cdot \eta' a_1),$$

d. h. wegen

$$\omega' - \omega = \frac{-\sqrt{D}}{a}, \quad \omega_1' - \omega_1 = \frac{-\sqrt{D}}{a_1}$$

diese andere:

$$a = (\alpha\delta - \beta\gamma) \cdot N(\eta) \cdot a_1$$

her; da aber nach Voraussetzung $a, a_1, N(\eta)$ positiv sind, folgt $\alpha\delta - \beta\gamma = +1$.

11. Weil hiernach das Bestehen einer Beziehung von der Art der Gleichung (56) zwischen den Idealen j, j_1 vollkommen gleichbedeutend ist mit der (eigentlichen) Äquivalenz der zugeordneten Formen, sollen hinfort zwei Ideale j, j_1, zwischen denen eine Beziehung (56) stattfindet, selbst einander (eigentlich) äquivalent heißen. Man sieht so die frühere Frage nach der Äquivalenz zweier Formen wieder unter einen neuen Gesichtspunkt gestellt, von dem aus ihre eigentlich arithmetische Bedeutung sichtbar wird. Durch die im vorigen festgehaltene Voraussetzung, wonach der erste Koeffizient der zu untersuchenden Formen positiv sein sollte, wird der Allgemeinheit der Untersuchung kein Abbruch getan. Denn man kann dabei eine Form $ax^2 + bxy + cy^2$, deren erster Koeffizient negativ wäre, leicht durch eine andere, ihr eigentlich äquivalente ersetzen, in welcher dies nicht der Fall ist. In der Tat, sei m irgend eine positive ganze Zahl, die durch (a, b, c) eigentlich darstellbar ist, wie es deren stets gibt, etwa $m = a\alpha^2 + b\alpha\gamma + c\gamma^2$, und seien β, δ so gewählt, daß $\alpha\delta - \beta\gamma = 1$ ist, so geht (a, b, c) durch die Substitution

$$x = \alpha x' + \beta y', \quad y = \gamma x' + \delta y'$$

(siehe vorigen Abschnitt, Kap. 5, Nr. 4 und 5) in eine ihr eigentlich äquivalente Form (m, r, n) mit positivem ersten Koeffizienten über, welche zur Untersuchung der Äquivalenz an Stelle von (a, b, c) gesetzt werden kann.

Die Beziehung (56) ist von der Art, daß zwei Ideale, welche demselben dritten Ideale äquivalent sind, es auch unter sich sind; denn aus zwei Gleichungen $j = \eta_1 \cdot j_1$,

$\mathfrak{j} = \eta_2 \cdot \mathfrak{j}_2$, worin η_1, η_2 zwei Zahlen des Körpers mit positiver Norm bedeuten, folgt $\eta_1 \mathfrak{j}_1 = \eta_2 \mathfrak{j}_2$, also

$$\mathfrak{j}_1 = \frac{\eta_2}{\eta_1} \cdot \mathfrak{j}_2 ,$$

wo nun auch $\frac{\eta_2}{\eta_1}$ eine Zahl des Körpers mit positiver Norm sein wird. Wenn man demnach sämtliche Ideale des Körpers, welche unter sich (eigentlich) äquivalent sind, stets in eine Klasse von Idealen zusammenfaßt, so muß jeder Idealklasse eine bestimmte Klasse äquivalenter Formen mit der Diskriminante D eindeutig zugeordnet sein, und umgekehrt, so daß die Anzahl der Idealklassen ebenso groß ist, wie die der Formenklassen. Da nun (vor. Abschn. Kap. 5, Nr. 16 und 20) nachgewiesen ist, daß die letztere nur endlich ist, dürfen wir den äußerst wichtigen **Satz** aussprechen:

Die Anzahl der Idealklassen ist endlich.

Wir heben diejenige Idealklasse als Hauptklasse hervor, welche der Hauptklasse der quadratischen Formen entspricht, deren Ideale nämlich mit $\mathfrak{g}$ äquivalent sind, so daß

$$\mathfrak{j} = \eta \cdot \mathfrak{g} = \eta \cdot [1, \theta] = [\eta, \eta \theta]$$

gesetzt werden kann. Da die Zahlen eines jeden Ideals ganze Zahlen des Körpers sind, muß insbesondere auch die im Modul zur Rechten enthaltene Zahl η selbst eine ganze Zahl sein. Ist diese Bedingung aber erfüllt, so bezeichnet in der Tat der Modul ein Ideal, da mit η und $\eta\theta$ zugleich

$$\eta(u + v\theta) = u \cdot \eta + v \cdot \eta\theta$$

und

$$\eta\theta(u + v\theta) = -\frac{D(D-1)}{4} v \cdot \eta + (u + vD) \cdot \eta\theta ,$$

mithin auch jedes Produkt $(\eta \cdot x + \eta\theta \cdot y)(u + v\theta)$ aus einer Zahl des Moduls in irgend eine ganze Zahl wieder eine Zahl des Moduls ist; ist also zudem noch die Norm von η positiv, so ist das Ideal äquivalent mit $\mathfrak{g}$. Man erkennt hieraus, daß alle Ideale der Hauptklasse und nur solche erhalten werden, wenn man $\mathfrak{g}$ mit allen ganzen Zahlen, deren Norm positiv ist, multipliziert. Sie sind also, wenn wir mit ζ eine solche Zahl bezeichnen, mit den Moduln $\zeta \cdot \mathfrak{g}$ oder, wie wir lieber schreiben wollen, mit $\mathfrak{g}\zeta$ identisch.

Derartige Ideale werden wir **Hauptideale** nennen. Setzt man $\zeta = u + v\theta$, so findet sich

$$\mathfrak{g}\zeta = \left[u + v\theta\,,\ \frac{-D(D-1)}{4}v + (u + Dv)\theta\right],$$

woraus nach (36)

$$\mathfrak{N}(\mathfrak{g}\zeta) = u(u + Dv) + \frac{D(D-1)}{4}v^2,$$

d. i.

$$(58) \qquad \mathfrak{N}(\mathfrak{g}\zeta) = N(\zeta)$$

hervorgeht.

12. Sind j_1, j_2 irgend zwei Ideale und bezeichnet ξ jede Zahl des ersten, η jede Zahl des zweiten von ihnen, so ist die Gesamtheit der Produkte $\xi\cdot\eta$ nicht notwendig wieder ein Zahlenmodul, wohl aber entsteht ein solcher, wenn man jener Gesamtheit noch alle durch Addition solcher Produkte entstehenden Zahlen hinzufügt. Sind nämlich z. B.

$$\xi\eta + \xi_1\eta_1\,, \qquad \xi_2\eta_2 + \xi_3\eta_3$$

irgend zwei so entstehende Zahlen, so ist ja auch ihre Summe

$$\xi\eta + \xi_1\eta_1 + \xi_2\eta_2 + \xi_3\eta_3$$

eine durch Addition von Produkten der angegebenen Art gebildete Zahl, nicht minder auch ihre Differenz

$$\xi\eta + \xi_1\eta_1 + (-\xi_2\eta_2) + (-\xi_3\eta_3),$$

da mit ξ_2, ξ_3 auch $-\xi_2, -\xi_3$ Zahlen in j_1 sind. Die gedachte Gesamtheit von Produkten und Summen von Produkten aus je einer Zahl in j_1 und je einer Zahl in j_2 hat also die charakteristische Eigenschaft eines Zahlenmoduls und zwar genauer diejenige eines Ideals; denn, bezeichnet ζ jede ganze Zahl des Körpers, so wird mit $\xi\eta + \xi_1\eta_1 + \ldots$ zugleich auch $\zeta(\xi\eta + \xi_1\eta_1 + \ldots) = \zeta\xi\cdot\eta + \zeta\xi_1\cdot\eta_1 + \ldots$ der gedachten Gesamtheit angehören, da $\zeta\xi, \zeta\xi_1, \ldots$ zugleich mit $\xi_1, \xi_2, \ldots$ Zahlen des Ideals j_1 sind. Wir werden die so definierte Gesamtheit J von Zahlen das Produkt der beiden Ideale nennen und

$$(59) \qquad J = j_1 \cdot j_2$$

setzen, und dürfen den **Satz** aussprechen: das Produkt zweier Ideale ist wieder ein Ideal.

Das Produkt eines Ideals j in das Ideal $\mathfrak{g}$ ist stets mit dem ersteren identisch:

(59 a) $$\mathfrak{g}j = j\,;$$

in der Tat gehört der Definition eines Ideals zufolge jedes Produkt aus einer Zahl in $\mathfrak{g}$ und einer Zahl in j, also auch jede Summe solcher Produkte wieder zu j, andererseits ist aber auch jede Zahl ξ in j, da sie gleich $1 \cdot \xi$ gesetzt werden kann und 1 in $\mathfrak{g}$ enthalten ist, eine Zahl des Produktes $\mathfrak{g}j$, und somit ist die Gesamtheit der Zahlen in $\mathfrak{g}j$ und diejenige der Zahlen in j ein- und dieselbe.

Seien nun j_1', j_2' zwei andere Ideale und

(60) $$J' = j_1' \cdot j_2'$$

ihr Produkt. Wenn j_1', j_2' den Idealen j_1, j_2 resp. äquivalent sind, so daß, unter η_1, η_2 zwei Zahlen in $\mathfrak{K}$ mit positiver Norm verstanden, $j_1' = \eta_1 \cdot j_1$, $j_2' = \eta_2 \cdot j_2$ gesetzt werden kann, so schließt man aus (59) und (60)

$$J' = \eta_1 \eta_2 \cdot J\,,$$

wo nun auch $\eta_1 \eta_2$ eine Zahl in $\mathfrak{K}$ mit positiver Norm sein wird, mithin die Äquivalenz der Ideale J, J' oder den

Satz: Sind C_1, C_2 zwei Idealklassen, so gehören die verschiedenen Ideale, die durch Multiplikation aus einem Ideale der ersten in ein Ideal der zweiten Klasse entstehen, sämtlich ein- und derselben Klasse K an. — Diese, somit nicht von der individuellen Auswahl der Ideale aus C_1 und C_2 abhängige, sondern allein von den Klassen C_1, C_2 selbst bestimmte Klasse K soll aus C_1 und C_2 zusammengesetzt heißen und als ihr Produkt geschrieben werden, wobei die Reihenfolge der Faktoren offenbar gleichgültig ist:

(61) $$K = C_1 \cdot C_2 = C_2 \cdot C_1\,.$$

Wird in solcher Weise eine Klasse C mit der Hauptklasse H zusammengesetzt, so entsteht wieder die Klasse C:

(61 a) $$H \cdot C = C\,;$$

denn, ist j ein Ideal in C, so gehört, da $\mathfrak{g}$ ein Ideal der Klasse H ist, $\mathfrak{g}j$ der Klasse $H \cdot C$ an, die keine andere sein kann als C, da $\mathfrak{g}j = j$ ist.

13. Sowohl die Multiplikation von Idealen als auch die Zusammensetzung ihrer Klassen kann ohne weiteres von zwei auf beliebig viel derselben ausgedehnt werden, und daraus geht der Sinn einer Formel wie diese:

$$K = C \cdot C_1 \cdot C_2 \ldots C_{n-1}$$

hervor. Sind dabei die einzelnen Klassen, aus denen K durch sukzessive Zusammensetzung entsteht, miteinander identisch, so schreibt man solche Formel auch in der Form

$$K = C^n$$

und nennt K die $n$te Potenz von C. Ebenso bezeichnet j^n das Ideal, welches durch die eben definierte Multiplikation aus n Faktoren j hervorgebracht wird.

Bildet man in dieser Weise für irgend eine Idealklasse C die aufeinanderfolgenden Potenzen $C, C^2, C^3, C^4, \ldots,$ so folgt aus der nur endlichen Anzahl verschiedener Idealklassen, daß jene nicht alle voneinander verschieden sein können, daß vielmehr einmal eine spätere C^{m+n} mit einer früheren C^m identisch sein muß:

$$(62) \qquad C^{m+n} = C^m \cdot C^n = C^m \text{ *)}.$$

Nun sei j irgend ein in C enthaltenes Ideal; dann findet sich in C^m, C^n, C^{m+n} resp. das Ideal j^m, j^n, j^{m+n}, und aus der Gleichheit (62) der Klassen C^m und $C^m \cdot C^n$ folgt die Äquivalenz der Ideale j^m und $j^m \cdot j^n$, d. i. eine Gleichung

$$(63) \qquad \eta \cdot j^m = j^m \cdot j^n,$$

in welcher η eine Zahl des Körpers $\mathfrak{K}$ mit positiver Norm bedeutet. Dies vorausgeschickt, bezeichne man mit α_1, α_2 eine Basis des Ideals j^m, mit β_1, β_2 eine Basis des Ideals j^n; dann sind die Produkte $\alpha_1 \beta_1, \alpha_2 \beta_1, \alpha_1 \beta_2, \alpha_2 \beta_2$ Zahlen

---

*) Daß in der Tat $C^{m+n} = C^m \cdot C^n$ gesetzt werden kann, ersieht man leicht, wenn man bedenkt, daß nach der Bildungsweise eines Idealproduktes

$$(j_1 j_2) \cdot j_3 = j_1 \cdot (j_2 j_3)$$

gesetzt werden kann; daraus folgt dann allgemeiner

$$j^m \cdot j^n = j^{m+n},$$

also auch die obige Gleichheit.

des Ideals $j^m \cdot j^n$, und da sie zufolge (63) auch in $\eta \cdot j^m$ enthalten sind, so ergeben sich Gleichungen von der Form

$$(64)\quad \begin{cases} \alpha_1 \beta_1 = \eta (x_1 \alpha_1 + x_2 \alpha_2), & \alpha_2 \beta_1 = \eta (y_1 \alpha_1 + y_2 \alpha_2) \\ \alpha_1 \beta_2 = \eta (x_1' \alpha_1 + x_2' \alpha_2), & \alpha_2 \beta_2 = \eta (y_1' \alpha_1 + y_2' \alpha_2) \end{cases}$$

mit ganzzahligen Koeffizienten $x_1, x_2, y_1, y_2, x_1', \ldots$ Schreibt man die beiden ersten in der Form

$$\alpha_1 \left(x_1 - \frac{\beta_1}{\eta}\right) + \alpha_2 x_2 = 0, \qquad \alpha_1 y_1 + \alpha_2 \left(y_2 - \frac{\beta_1}{\eta}\right) = 0,$$

so erhält man durch Elimination von α_1, α_2 aus ihnen die Beziehung

$$\left(x_1 - \frac{\beta_1}{\eta}\right)\left(y_2 - \frac{\beta_1}{\eta}\right) - x_2 y_1 = 0$$

oder

$$\left(\frac{\beta_1}{\eta}\right)^2 - (x_1 + y_2) \cdot \frac{\beta_1}{\eta} + x_1 y_2 - x_2 y_1 = 0,$$

d. h. $\frac{\beta_1}{\eta}$ ist Wurzel einer quadratischen Gleichung mit ganzzahligen Koeffizienten, deren erster gleich 1 ist, also eine offenbar im Körper $\mathfrak{K}$ enthaltene ganze algebraische Zahl γ_1. In gleicher Weise schließt man aus den beiden letzten Gleichungen (64), daß $\frac{\beta_2}{\eta}$ eine ganze algebraische Zahl γ_2 des Körpers $\mathfrak{K}$ ist. Demnach ist

$$j^n = [\beta_1, \beta_2] = \eta \cdot [\gamma_1, \gamma_2]$$

und aus (63) folgt

$$[\alpha_1, \alpha_2] = [\alpha_1, \alpha_2] \cdot [\gamma_1, \gamma_2].$$

Nun sind offenbar alle Zahlen des rechtsstehenden Produkts von der Form

$$x_1 \cdot \alpha_1 \gamma_1 + x_2 \cdot \alpha_1 \gamma_2 + x_3 \cdot \alpha_2 \gamma_1 + x_4 \cdot \alpha_2 \gamma_2$$

mit ganzzahligen Koeffizienten x_1, x_2, x_3, x_4; zufolge der vorstehenden Gleichung haben diese Form also auch alle Zahlen des Moduls $[\alpha_1, \alpha_2]$, insbesondere darf man demnach setzen

$$\alpha_1 = x_1' \cdot \alpha_1 \gamma_1 + x_2' \cdot \alpha_1 \gamma_2 + x_3' \cdot \alpha_2 \gamma_1 + x_4' \cdot \alpha_2 \gamma_2$$
$$\alpha_2 = x_1'' \cdot \alpha_1 \gamma_1 + x_2'' \cdot \alpha_1 \gamma_2 + x_3'' \cdot \alpha_2 \gamma_1 + x_4'' \cdot \alpha_2 \gamma_2$$

und erhält, wenn man α_1, α_2 aus diesen beiden Gleichungen eliminiert, die folgende Beziehung:

$$1 = (x_3'\gamma_1 + x_4'\gamma_2)(x_1''\gamma_1 + x_2''\gamma_2) - (x_1'\gamma_1 + x_2'\gamma_2)(x_3''\gamma_1 + x_4''\gamma_2)$$
$$+ x_1'\gamma_1 + x_2'\gamma_2 + x_3''\gamma_1 + x_4''\gamma_2\,;$$

da aber die hier auftretenden Produkte als Produkte einer ganzen Zahl in eine Zahl des Moduls $[\gamma_1, \gamma_2]$, der offenbar ebenso wie $[\beta_1, \beta_2]$ ein Ideal ist, wieder Zahlen des letzteren und daher die ganze rechte Seite der vorigen Gleichung eine solche Zahl ist, so findet sich 1 als eine im Ideale $[\gamma_1, \gamma_2]$ enthaltene Zahl.

Das einzige Ideal aber, welches die Zahl 1 enthält, ist das Ideal $\mathfrak{g}$. Denn, da jedes Ideal $\mathfrak{j}$ die Form (49) hat, derzufolge sa die kleinste in ihm enthaltene rationale ganze Zahl ist, muß, wenn es die Zahl 1 enthält, $sa = 1$, d. h. $s = a = 1$ und somit

$$\mathfrak{j} = [1, \omega] = [1, h + \theta] = [1, \theta] = \mathfrak{g}$$

sein. — Hieraus schließt man für unsere Betrachtung, daß $[\gamma_1, \gamma_2] = \mathfrak{g}$ mithin $\mathfrak{j}^n = \eta \cdot \mathfrak{g}$, d. h. äquivalent mit $\mathfrak{g}$ oder ein Hauptideal, und daher die Klasse C^n, der es angehört, die Hauptklasse ist.

Auf diese Weise ist folgendes Ergebnis gewonnen:

Für jede Idealklasse C gibt es eine gewisse Potenz C^n, welche mit der Hauptklasse H identisch ist. Allgemeiner ist dann für jedes positive ganzzahlige q

$$C^{qn} = H^q = H.$$

Man schließt weiter, daß es zu jeder Klasse C eine Klasse C' gibt, die mit ihr zusammengesetzt die Hauptklasse gibt, nämlich $C' = C^{n-1}$. Es gibt aber auch nur eine solche Klasse. Wäre nämlich

$$C \cdot C_1 = H, \quad C \cdot C_2 = H,$$

so ergäbe sich

$$C \cdot C_1 = C \cdot C_2\,,$$

aus jeder solchen Beziehung zwischen Idealklassen folgt aber stets die Gleichheit $C_1 = C_2$, denn, multipliziert man sie mit C^{n-1} und beachtet die Gleichung $C^n = H$, so erhält man $H \cdot C_1 = H \cdot C_2$, d. i. aber wegen (61a) die Gleichheit $C_1 = C_2$. Die somit völlig eindeutig definierte Idealklasse C' heiße die Reziproke zu C.

14. Unter allen Potenzen von C, welche mit H identisch sind, wird eine die niedrigste sein; nennen wir diese Potenz C^e, so soll e der Exponent heißen, zu welchem die Klasse C gehört. Man überzeugt sich unschwer, daß er ein Teiler von der Anzahl h aller Idealklassen ist. Dies wäre der Fall, wenn $e=h$, d. h. mit den verschiedenen Potenzen

$$(65) \qquad C,\ C^2,\ C^3,\ \ldots\ C^e$$

die Gesamtheit der Idealklassen erschöpft wäre. Ist aber $e<h$, so sei C_1 eine der übrigen Idealklassen, und man bilde die Produkte

$$(66) \qquad CC_1,\ C^2C_1,\ C^3C_1,\ \ldots,\ C^eC_1\,.$$

Diese sind erstens verschieden von den Klassen (65), denn bezeichnen m, μ zwei Zahlen $\lesseqgtr e$, so folgte aus $C^m \cdot C_1 = C^\mu$ die Gleichung

$$C^e \cdot C_1 \quad \text{d. i.} \quad H \cdot C_1 = C_1 = C^{e+\mu-m}\,;$$

setzt man nun $e+\mu-m = q\cdot e + r$, wo $r \lesseqgtr e$ den kleinsten positiven Rest (mod. e) bedeutet, so wird

$$C^{e+\mu-m} = C^{qe} \cdot C^r = H \cdot C^r = C^r\,,$$

und somit wäre C_1 gegen die Voraussetzung eine der Klassen (65). Die Produkte (66) bezeichnen aber zweitens auch lauter untereinander verschiedene Klassen, denn wären zwei nicht identische dieser Produkte gleich, etwa $C^m \cdot C_1 = C^\mu \cdot C_1$, so erschlösse man aus dieser Gleichung nach Ende voriger Nummer die Gleichheit $C^m = C^\mu$, d. i. die Identität der Produkte gegen die Voraussetzung. Demnach gibt es mindestens die $2e$ Klassen (65) und (66). Ist aber außer ihnen noch weiter eine Klasse C_2 vorhanden, so liefert die Reihe

$$(67) \qquad C\cdot C_2,\ C^2\cdot C_2,\ C^3\cdot C_2,\ \ldots,\ C^e\cdot C_2\,,$$

wie nun auf gleiche Weise zu erkennen ist, e sowohl unter sich, als von den Klassen (65) verschiedene Klassen; sie sind aber endlich auch von den Klassen (66) verschieden, da aus einer Gleichung $C^\mu \cdot C_2 = C^m \cdot C_1$ die andere:

$$C^e \cdot C_2 \quad \text{d. i.} \quad H \cdot C_2 = C_2 = C^{e+m-\mu} \cdot C_1$$

oder, wenn $e+m-\mu = qe+r$ gesetzt und $r \lesseqgtr e$ gedacht wird, die Gleichung $C_2 = C^r \cdot C_1$ d. h. gegen die Voraussetzung C_2 als eine der Klassen (66) sich ergäbe. Ist nun außer

den $3e$ Klassen (65), (66), (67) noch eine weitere vorhanden, so treten ebenso wieder gleich e neue Klassen hinzu, usw., bis alle Idealklassen erschöpft sind und deren Anzahl h als ein Vielfaches von e hervorgeht.

Setzt man demgemäß $h = q \cdot e$, so liefert die Bemerkung gegen Ende voriger Nummer die Gleichung

$$C^h = H \tag{68}$$

oder den **Satz:** Bedeutet h die Anzahl der Idealklassen, so ist die $h$te Potenz jeder Idealklassse mit der Hauptklasse identisch.

Diesem Satze völlig gleichbedeutend ist der andere Ausspruch: daß die $h$te Potenz eines jeden Ideals j ein Hauptideal:

$$j^h = \mathfrak{g}\,\zeta \tag{69}$$

ist. Hieraus fließt wieder ein neuer **Satz,** dessen fundamentale Wichtigkeit für die Arithmetik des Körpers $\mathfrak{K}$ sehr bald erhellen wird, und der sich aussprechen läßt, wie folgt:

Zu jedem Ideal j gibt es ein Ideal j_1 von solcher Beschaffenheit, daß das Produkt $j \cdot j_1$ ein Hauptideal wird. In der Tat leistet das Ideal $j_1 = j^{h-1}$ jedenfalls dieser Forderung Genüge.

Zweites Kapitel.

Die Einheiten des quadratischen Körpers.

1. Indem wir uns nun dazu wenden, die einzelnen ganzen Zahlen des Körpers $\mathfrak{K}$ für sich zu betrachten, um sie auf ihre arithmetischen Eigenschaften zu prüfen, wird es sich wesentlich um ihre Teilbarkeit, insbesondere um die Frage handeln, ob im Körper $\mathfrak{K}$ die gleichen Gesetze der Teilbarkeit wie im rationalen Zahlenkörper, z. B. die eindeutige Zerlegung jeder Zahl in Primfaktoren, in Gültigkeit bleiben oder nicht, und wie etwa sie im letzteren Falle zu ersetzen sind.

Wir nennen aber eine ganze Zahl ζ des Körpers $\mathfrak{K}$ teilbar durch eine andere ganze Zahl ξ desselben, wenn eine ganze algebraische Zahl η vorhanden

ist der Art, daß $\zeta = \xi \cdot \eta$ gesetzt werden kann. Da hieraus $\eta = \frac{\zeta}{\xi}$ folgt, so muß die gedachte Zahl η dem Körper $\mathfrak{K}$ angehören, also ebenfalls eine ganze Zahl dieses Körpers sein. Sind nun etwa

$$\zeta = r + s\theta, \quad \xi = t + u\theta, \quad \eta = v + w\theta,$$

mithin

$$r + s\theta = (t + u\theta)(v + w\theta),$$

wo $\theta = \frac{D + \sqrt{D}}{2}$, so muß diese Gleichung bestehen bleiben, wenn $\sqrt{D}$ in $-\sqrt{D}$, d. h. θ und damit ζ, ξ, η in die konjugierten Zahlen θ', ζ', ξ', η' verwandelt werden; aus $\zeta = \xi \cdot \eta$ folgt daher $\zeta' = \xi' \cdot \eta'$ und folglich auch

$$(1) \qquad N(\zeta) = N(\xi\eta) = N(\xi) \cdot N(\eta).$$

Die Normen ganzer Zahlen sind aber rationale ganze Zahlen, denn nach Nr. 2 vorigen Kapitels sind sie rational, als Produkt zweier (konjugierter) ganzer algebraischer Zahlen aber (nach Nr. 4 das.) selbst ganze algebraische Zahlen und daher (ebendas.) **rationale** ganze Zahlen. Ist demnach keine der Zahlen ξ, η eine solche, deren Norm gleich ± 1, so müssen $N(\xi)$, $N(\eta)$ ganze von ± 1 verschiedene Zahlen kleiner als $N(\zeta)$ sein. Nennt man nun, wenn ζ durch ξ teilbar oder ein Vielfaches von ξ, oder letztere Zahl ein Teiler von ζ ist, die Darstellung von ζ in der Form $\zeta = \xi \cdot \eta$ eine **Zerlegung** von ζ in **Faktoren**, so geht aus der letzten Bemerkung unmittelbar hervor, daß eine ganze Zahl ζ nur in eine endliche Anzahl von Faktoren zerlegbar ist, deren Normen von ± 1 verschieden sind. Denn andernfalls zerfiele ihre Norm $N(\zeta)$ in eine unbegrenzte Menge von kleineren und von ± 1 verschiedenen ganzzahligen Faktoren, was für eine rationale ganze Zahl bekanntlich nicht möglich ist. So ist als erstes wichtiges allgemeines Ergebnis der **Satz** gewonnen:

Jede ganze Zahl ζ des Körpers $\mathfrak{K}$ ist entweder unzerlegbar oder nur in eine endliche Anzahl von Faktoren zerlegbar, wenn man von solchen Faktoren absieht, deren Norm gleich ± 1 ist.

Zwei ganze Zahlen ξ und $\zeta = \xi \cdot \eta$, die sich nur um einen Faktor η mit der Norm ± 1 unterscheiden, sollen **assoziiert** heißen. Kennt man die Zerlegung einer dieser Zahlen in Faktoren, deren Normen von ± 1 verschieden sind, so hat man damit offenbar diese Zerlegung auch für jede ihr assoziierte Zahl; um also für jede Zahl des Körpers jene Zerlegungen zu finden, bedarf es nur deren Auffindung für je eine Zahl aus jeder Gruppe von assoziierten Zahlen; zur Bildung dieser letzteren aber hat man die Kenntnis aller ganzen Zahlen η des Körpers nötig, für welche

(2) $$N(\eta) = \pm 1$$

ist. Diese Zahlen sollen **Einheiten** genannt werden. Sie können auch als die Teiler der Zahl 1 definiert werden; in der Tat, besteht die Gleichung (2), d. h. $1 = \pm \eta' \cdot \eta$, so ist η, da auch die konjugierte Zahl η' eine ganze Zahl ist, ein Teiler von 1; umgekehrt, wenn η ein Teiler von 1, also $1 = \eta \cdot \eta_1$ ist, während η_1 eine ganze Zahl bedeutet, so ist auch $N(\eta) \cdot N(\eta_1) = 1$, mithin die ganze rationale Zahl $N(\eta) = \pm 1$. Demnach ist durch eine Einheit η des Körpers jede ganze Zahl ζ desselben teilbar, denn aus $\zeta = 1 \cdot \zeta$ und $1 = \eta \cdot \eta_1$ folgt $\zeta = \eta \cdot \eta_1 \zeta$, wo $\eta_1 \zeta$ eine ganze Zahl, und umgekehrt wird eine ganze Zahl des Körpers, durch welche jede seiner Zahlen, also auch die Zahl 1 teilbar ist, eine Einheit sein.

2. Wir richten nun zunächst unsere Bemühung darauf, alle Einheiten des Körpers zu ermitteln. Es genügt, alle diejenigen zu finden, deren Norm $+1$ ist, die wir hinfort ausschließlich als Einheiten betrachten wollen, während diejenigen mit der Norm -1 etwa als **Halbeinheiten** bezeichnet werden mögen. Kennt man nämlich die ersteren, die mit ε bezeichnet seien, und gibt es überhaupt in $\mathfrak{K}$ eine Einheit η mit der Norm -1, so erhält man aus dieser einen sämtliche übrigen durch den Ausdruck $\eta \cdot \varepsilon$; in der Tat ist einerseits $\eta \varepsilon$ eine solche, da $N(\eta \varepsilon) = N(\eta) \cdot N(\varepsilon) = -1$; ist aber η_1 irgend eine der Halbeinheiten und η' die Konjugierte von η, so daß $\eta \cdot \eta' = -1$, so ist $\varepsilon = -\eta' \cdot \eta_1$ eine Einheit mit der Norm $N(\varepsilon) = N(-1) \cdot N(\eta') \cdot N(\eta_1) = +1$, und somit $\eta_1 = -\eta \eta' \cdot \eta_1 = \eta \cdot \varepsilon$ von der zuvor bezeichneten Form.

Nun hat jede der gesuchten Zahlen ε als ganze Zahl

des Körpers die Form $\varepsilon = x + y\theta$, und es ergibt sich zur Bestimmung der Zahlen x, y die Bedingungsgleichung

$$(3)\qquad N(\varepsilon) = N(x + y\theta) = \left(\frac{2x + Dy}{2}\right)^2 - D \cdot \frac{y^2}{4} = 1\,.$$

Sie nimmt, falls $D = 4d$ ist, die Gestalt

$$N(\varepsilon) = X^2 - dY^2 = 1\,,$$

worin $X = x + 2dy$, $Y = y$, und falls $D = d = 4\delta + 1$ ist, die Gestalt

$$N(\varepsilon) = X^2 + XY + \frac{1-d}{4}Y^2 = 1$$

an, worin $X = x + 2\delta y$, $Y = y$ gedacht ist. Da nach diesen Beziehungen aus ganzzahligen x, y sich auch ganzzahlige X, Y ergeben und umgekehrt, so sind die Einheiten ε und die Darstellungen der Eins durch die jedesmalige Hauptform mit der Diskriminante D einander eindeutig zugeordnet. — Aus (3) ergibt sich ferner die Gleichung

$$(4)\qquad t^2 - Du^2 = 4\,,$$

wo

$$(5)\qquad t = 2x + Dy\,,\qquad u = y$$

gesetzt ist. Jede Einheit ε liefert also durch die Gleichungen (5) eine ganzzahlige Lösung der Gleichung (4). Aber auch umgekehrt; bedeuten nämlich t, u irgend eine ganzzahlige Lösung dieser Gleichung, so sind, wenn $D = d = 4\delta + 1$, entweder beide Zahlen t, u gerade oder beide ungerade; ist aber $D = 4d$, so muß t gerade sein; in allen Fällen liefern dann aber die Formeln (5) ganzzahlige Werte $x = \dfrac{t - Du}{2}$, $y = u$, also eine ganze Zahl

$$(6)\qquad \varepsilon = x + y\theta = \frac{t + u\sqrt{D}}{2}$$

mit der Norm $+1$. Hiernach kommt die Aufgabe, alle Einheiten ε des Körpers zu finden, auf die andere zurück, alle ganzzahligen Auflösungen der Gleichung (4) zu ermitteln. Letztere Aufgabe ist zuerst von *Fermat* gestellt und behandelt worden, und so sollte die Gleichung (4) wohl *Fermat*sche Gleichung genannt werden, doch heißt sie gewöhnlich *Pell*sche Gleichung, wie *Euler* sie getauft hat, in-

dem er irrtümlicherweise dem Engländer *Pell* besondere Verdienste um sie zuschrieb, die ihm nicht zukommen. Im Falle einer negativen Diskriminante D hat sie offenbar nur eine endliche Anzahl ganzzahliger Lösungen. Setzt man nämlich $D = -\Delta$, so daß Δ den Absolutwert von D bezeichnet, so nimmt die Gleichung (4) die Form an

$$t^2 + \Delta u^2 = 4\,. \tag{4a}$$

Ist $D \equiv 1 \pmod{4}$, so wird $\Delta \equiv 3 \pmod{4}$; vorstehende Gleichung hat mithin nur die zwei Lösungen $t = \pm 2$, $u = 0$, wenn $\Delta > 3$; falls aber $\Delta = 3$, d. h. $D = -3$, noch die vier Lösungen $t = \pm 1$, $u = \pm 1$. Ist dagegen $D \equiv 0 \pmod{4}$, so hat (4a) wieder nur zwei Lösungen $t = \pm 2$, $u = 0$, wenn $\Delta > 4$; falls aber $\Delta = 4$, also $D = -4$ ist, noch die zwei Lösungen $t = 0$, $u = \pm 1$. Im Körper $\mathfrak{K}$ gibt es also, falls seine Grundzahl $D < 0$ ist, im allgemeinen nur die beiden rationalen Einheiten ± 1; nur, wenn $D = -4$ ist, kommen zu diesen noch die Einheiten $\pm i$, wenn aber $D = -3$ ist, die Einheiten $\frac{1 \pm \sqrt{-3}}{2}$ und $-\frac{1 \pm \sqrt{-3}}{2}$ hinzu.

Ganz anders im Falle einer positiven Grundzahl D: in diesem ist die Anzahl der Einheiten oder der Auflösungen der *Pell*schen Gleichung unendlich groß. Man sieht leicht ein, daß dies der Fall ist, wenn nur überhaupt eine, von der selbstverständlichen Lösung $t = \pm 2$, $u = 0$ verschiedene Lösung vorhanden ist; aber der Nachweis, daß letzteres immer der Fall ist, hat den Mathematikern früherer Periode große Mühe gekostet und ist erst *Lagrange* gelungen. Aus den Betrachtungen des Kapitel 5 vorigen Abschnitts (Nr. 18—20) entnehmen wir leicht sowohl diese Tatsache, als auch eine Methode, sämtliche Lösungen der Gleichung zu finden.

3. Sei nämlich unter der Voraussetzung $D > 0$

$$\omega_0 = \frac{-b + \sqrt{D}}{2a} \tag{7}$$

irgend eine reduzierte Zahl der in Nr. 18 mit Ω bezeichneten Gesamtheit, also Wurzel einer Gleichung

$$az^2 + bz + c = 0 \tag{8}$$

mit der Diskriminante $D = b^2 - 4ac$, wobei $a > 0$ und a, b, c ganze Zahlen ohne gemeinsamen Teiler sind. Der Kettenbruch für ω_0, welcher rein periodisch ist, sei

(9) $$\omega_0 = K(q_0, q_1, q_2, \ldots, q_{k-1}, \omega_0),$$

also k die Anzahl der Glieder der (kleinsten) Periode. Bezeichnen dann $\frac{z_0}{n_0} = \frac{1}{0}$, $\frac{z_1}{n_1} = \frac{q_0}{1}$, $\frac{z_2}{n_2}, \ldots, \frac{z_k}{n_k}$ die ersten $k+1$ Näherungsbrüche, so besteht die Beziehung

$$\omega_0 = \frac{z_k \omega_0 + z_{k-1}}{n_k \omega_0 + n_{k-1}}$$

und allgemeiner die folgende:

(10) $$\omega_0 = \frac{z_h \omega_0 + z_{h-1}}{n_h \omega_0 + n_{h-1}},$$

wenn h ein beliebiges Vielfaches von k bedeutet. Daraus folgt aber

$$n_h \cdot \omega_0^2 + (n_{h-1} - z_h)\,\omega_0 - z_{h-1} = 0,$$

eine Gleichung, welche mit der anderen:

$$a \cdot \omega_0^2 + b \cdot \omega_0 + c = 0,$$

welcher ω_0 genügt, übereinstimmen muß, indem die Koeffizienten jener Gleichung nur um einen Proportionalitätsfaktor von den Koeffizienten dieser verschieden sein können. Bezeichnet nämlich u den größten gemeinsamen Teiler von n_h, $n_{h-1} - z_h$, z_{h-1}, so muß

(11) $$n_h = au, \quad n_{h-1} - z_h = bu, \quad z_{h-1} = -cu$$

sein; setzt man noch

(12) $$n_{h-1} + z_h = t,$$

so ergibt sich aus diesen Gleichungen

(13) $$z_h = \frac{t - bu}{2}, \quad n_h = au, \quad z_{h-1} = -cu, \quad n_{h-1} = \frac{t + bu}{2}.$$

Da aber bekanntlich

$$z_h n_{h-1} - n_h z_{h-1} = (-1)^h$$

ist, erschließt man für die ganzen Zahlen t, u durch Substitution vorstehender Werte folgende Beziehung:

$$\frac{t^2 - b^2 u^2}{4} + a c u^2 = \frac{t^2 - D u^2}{4} = (-1)^h .$$

Somit liefert die Gleichung (10) für jeden Index h, der ein Vielfaches der Periodenzahl k ist, vermittels der Formeln (11) und (12) eine ganzzahlige Auflösung der Gleichung

$$(14) \qquad t^2 - D u^2 = (-1)^h \cdot 4 .$$

Ist k und daher stets auch h gerade, so gewinnt man demnach für jedes Vielfache h von k, d. h. wenn man den Kettenbruch mit dem auf irgend eine Wiederholung der Periode folgenden Schlußnenner abbricht, eine ganzzahlige Auflösung der *Pell*schen Gleichung; ist dagegen die Periodenzahl k ungerade, so geschieht dies nur für jedes gerade Vielfache h von k, d. h. wenn der Kettenbruch mit dem auf eine gerade Anzahl Perioden folgenden Schlußnenner abgebrochen wird. In beiden Fällen aber ergeben die unendlich vielen zulässigen Werte von h eine unbegrenzte Menge von Auflösungen, die verschieden voneinander sein müssen, weil Zähler und Nenner der Näherungsbrüche mit deren Index wachsen, also wegen (12) auch t und damit zugleich auch u stets wachsende Werte erhalten.

4. Man überzeugt sich aber leicht, daß auf solche Weise auch sämtliche ganzzahlige Auflösungen der *Pell*schen Gleichung erhalten werden können. Es genügt zu zeigen, daß die angegebene Methode alle Auflösungen in positiven ganzen Zahlen t, u liefert, denn, abgesehen von den beiden evidenten Auflösungen $t = \pm 2$, $u = 0$, können stets vier Auflösungen

$$(15) \qquad t, u; \quad -t, u; \quad t, -u; \quad -t, -u$$

zusammengestellt werden, die aus der ersten durch bloße Veränderung der Vorzeichen hervorgehen, mit dieser Auflösung in positiven ganzen Zahlen also zugleich gegeben sind. Sei also t, u irgend eine Auflösung in positiven ganzen Zahlen; aus der Gleichung

$$(16) \qquad t^2 - D u^2 = 4 ,$$

welche in der Gestalt

$$\text{(16a)} \qquad \frac{t+u\sqrt{D}}{2} \cdot \frac{t-u\sqrt{D}}{2} = 1$$

geschrieben werden kann, folgt, daß mit $\frac{t+u\sqrt{D}}{2}$ auch $\frac{t-u\sqrt{D}}{2}$ positiv ist, und da wegen $u > 0$ die beiden Faktoren ungleich sind, muß $\frac{t+u\sqrt{D}}{2} > 1$, $\frac{t-u\sqrt{D}}{2} < 1$ sein. Ferner müssen wegen (16) t, Du zugleich gerade oder zugleich ungerade sein, und da $b \equiv D \pmod{2}$ ist, gilt das gleiche auch von t, bu. Setzt man also

$$\text{(17)} \quad A = \frac{t-bu}{2}, \quad \Gamma = au, \quad B = -cu, \quad \Delta = \frac{t+bu}{2},$$

so stellen A, B, Γ, Δ ganze Zahlen vor, welche mit Rücksicht auf (16) der Bedingung

$$\text{(18)} \qquad A\Delta - B\Gamma = 1$$

Genüge leisten. Hieraus folgen nun

$$\Gamma = au, \quad \Delta - A = bu, \quad -B = cu,$$

und die Gleichung

$$a\omega_0^2 + b\omega_0 + c = 0$$

läßt sich schreiben in der Form

$$\Gamma\omega_0^2 + (\Delta - A)\omega_0 - B = 0$$

und ergibt die Beziehung

$$\text{(19)} \qquad \omega_0 = \frac{A\omega_0 + B}{\Gamma\omega_0 + \Delta}.$$

Da aber ω_0 eine reduzierte Zahl ist, gelten die Ungleichheiten

$$0 < b + \sqrt{D} < 2a < -b + \sqrt{D},$$

denen man durch Multiplikation mit $-b + \sqrt{D}$ bzw. mit $b + \sqrt{D}$ auch folgende Form geben kann:

$$0 < b + \sqrt{D} < -2c < -b + \sqrt{D}.$$

Aus ihnen folgt zunächst $b < 0$, also $A > 0$. Ferner ist $b > -\sqrt{D}$, $2a - b > \sqrt{D}$, $2c - b > -\sqrt{D}$, daher

$$\varDelta = \frac{t + bu}{2} > \frac{t - u\sqrt{D}}{2} > 0,$$

$$A - B = \frac{(2c - b)u + t}{2} > \frac{t - u\sqrt{D}}{2} > 0,$$

$$\varGamma - \varDelta = \frac{(2a - b)u - t}{2} > \frac{u\sqrt{D} - t}{2},$$

d. h. größer als der negative echte Bruch

$$\frac{Du^2 - t^2}{2(u\sqrt{D} + t)} = \frac{-2}{t + u\sqrt{D}};$$

da aber $\varGamma - \varDelta$ eine ganze Zahl ist, muß $\varGamma - \varDelta \gtreqless 0$, $\varGamma \gtreqless \varDelta > 0$ sein. Aus $A\varDelta - 1 = B\varGamma$ folgt endlich $B\varGamma \gtreqless 0$, mithin auch $B \gtreqless 0$, und da es nicht gleich Null sein kann, so ist $B > 0$. Dies vorausgeschickt, entwickle man den positiven Bruch $\frac{A}{\varGamma}$ in einen Kettenbruch:

$$\frac{A}{\varGamma} = \lfloor p_0, p_1, p_2, \ldots, p_{h-1} \rceil,$$

was bekanntlich stets so eingerichtet werden kann, daß die Anzahl h der Teilnenner gerade ist. Wird unter $\frac{A'}{\varGamma'}$ der vorletzte Näherungsbruch verstanden, so besteht die Gleichung

$$A\varGamma' - A'\varGamma = 1.$$

Vergleicht man sie mit der Gleichung (18) und beachtet, daß B, $\varDelta$ ebenso wie A', $\varGamma'$ positiv und kleiner sind als resp. A, $\varGamma$, so ergibt sich nach Kapitel 4 Nr. 3 die Gleichheit von B mit A' und von $\varDelta$ mit $\varGamma'$ und die Formel (19) geht über in

$$\omega_0 = \frac{A\omega_0 + A'}{\varGamma\omega_0 + \varGamma'}$$

und ergibt die Gleichung

$$\omega_0 = \lfloor p_0, p_1, p_2, \ldots, p_{h-1}, \omega_0 \rceil,$$

der zufolge die Reihe der Teilnenner $p_0, p_1, p_2, \ldots, p_{k-1}$ notwendig mit den Gliedern der Periode $q_0, q_1, q_2, \ldots, q_{k-1}$ des Kettenbruchs (9) oder mit einer mehrfachen Wiederholung dieser Periode identisch sein muß. Die Zahlen A, B, Γ, Δ stimmen daher mit den Zahlen (13) überein, und die Auflösung t, u der *Pell*schen Gleichung ist also eine derjenigen, welche durch die zuvor bezeichnete Methode gewonnen werden können, w. z. b. w.

5. Wie schon bemerkt, fallen die so erhaltenen t, u um so größer aus, je größer h gewählt wird; daher findet man die Auflösung der *Pell*schen Gleichung in den kleinsten positiven Zahlen, wenn man den Kettenbruch (9), je nachdem k gerade oder ungerade ist, bei dem auf die erste bzw. auf die zweite Periode folgenden Schlußnenner abbricht. Kennt man aber diese Auflösung in den kleinsten positiven Zahlen, die wir τ, v nennen wollen, so sind dadurch mittelbar auch alle übrigen Auflösungen gegeben, denn es läßt sich eine allgemeine Formel aufstellen, durch welche alle Auflösungen mittels jener einen bestimmt werden.

Hierzu bemerke man folgendes. Stellt man die den vier Auflösungen (15) entsprechenden Einheiten

$$\frac{t+u\sqrt{D}}{2}, \quad \frac{t-u\sqrt{D}}{2}, \quad \frac{-t+u\sqrt{D}}{2}, \quad \frac{-t-u\sqrt{D}}{2}$$

auf, so ist von ihnen die erste die einzige, welche positiv und größer als Eins ist; in der Tat wegen (16a) ist $\frac{t-u\sqrt{D}}{2}$ zwar auch positiv, aber kleiner als Eins, während die beiden anderen negativ sind.

Da nun $\frac{t+u\sqrt{D}}{2}$ mit t, u zugleich wächst, so wird von allen positiven Einheiten, die zugleich größer als 1 sind, $\varepsilon_1 = \frac{\tau+v\sqrt{D}}{2}$ die kleinste sein. Weil aber $\frac{\tau+v\sqrt{D}}{2} > 1$, so wird die Potenz

$$\varepsilon_1^n = \left(\frac{\tau+v\sqrt{D}}{2}\right)^n$$

mit positiv wachsendem Exponenten n über jede Grenze hinaus wachsen. Sie stellt aber für jeden solchen Exponenten

eine Einheit dar, denn das Produkt zweier Einheiten ε, η ist stets wieder eine Einheit, da aus zwei Gleichungen $\varepsilon\varepsilon' = 1$, $\eta\eta' = 1$ sich $\varepsilon\eta \cdot \varepsilon'\eta' = 1$ ergibt; zugleich gibt ε_1^n die sämtlichen Einheiten, welche positiv und größer als 1 sind. In der Tat, wäre eine solche

$$\varepsilon = \frac{t + u\sqrt{D}}{2}$$

keiner Potenz von ε_1 gleich, so müßte sie notwendig zwischen zwei aufeinanderfolgende fallen, so daß Ungleichheiten bestünden von der Form

$$\left(\frac{\tau + v\sqrt{D}}{2}\right)^n < \frac{t + u\sqrt{D}}{2} < \left(\frac{\tau + v\sqrt{D}}{2}\right)^{n+1},$$

aus deren Multiplikation mit dem positiven Werte $\left(\frac{\tau - v\sqrt{D}}{2}\right)^n$ mit Rücksicht auf die Gleichung $\tau^2 - Dv^2 = 4$ die folgenden:

$$1 < \left(\frac{\tau - v\sqrt{D}}{2}\right)^n \cdot \frac{t + u\sqrt{D}}{2} < \frac{\tau + v\sqrt{D}}{2}$$

hervorgingen; der in der Mitte stehende Ausdruck stellt aber, wie bemerkt, wieder eine Einheit dar, die zudem den Ungleichheiten zufolge positiv und größer als 1, zugleich aber kleiner wäre als die kleinste dieser Einheiten ε_1. Aus diesem Widerspruch erkennt man, daß alle positiven Einheiten, welche größer sind als 1, mit den positiven Potenzen von ε_1 identisch sind, so daß gesetzt werden kann

$$\frac{t + u\sqrt{D}}{2} = \left(\frac{\tau + v\sqrt{D}}{2}\right)^n, \quad (n > 0).$$

Hieraus finden sich aber dem oben Gesagten gemäß die übrigen Einheiten

$$\frac{t - u\sqrt{D}}{2} = \left(\frac{t + u\sqrt{D}}{2}\right)^{-1} = \left(\frac{\tau + v\sqrt{D}}{2}\right)^{-n},$$

$$\frac{-t + u\sqrt{D}}{2} = -\left(\frac{\tau + v\sqrt{D}}{2}\right)^{-n}, \quad \frac{-t - u\sqrt{D}}{2} = -\left(\frac{\tau + v\sqrt{D}}{2}\right)^n.$$

Also ergibt sich folgender **Satz:**

Bei positiver Grundzahl enthält der Körper $\mathfrak{K}$ unendlich viel von ± 1 verschiedene Einheiten ε, welche sämtlich

durch eine Fundamentaleinheit $\varepsilon_1 = \frac{\tau + v\sqrt{D}}{2}$ mittels der Formel

(20) $$\varepsilon = \pm\left(\frac{\tau + v\sqrt{D}}{2}\right)^n$$

gegeben werden, wenn darin n alle positiven und negativen ganzen Zahlen durchläuft. Die Formel ergibt auch die beiden einzigen rationalen Einheiten ± 1 des Körpers, wenn man jenen Werten des n die Null noch hinzufügt.

Da nun andererseits alle Einheiten ε durch die Formel (6) geliefert wurden, wenn in dieser t, u sämtliche ganzzahligen Auflösungen der *Pell*schen Gleichung durchlaufen, so gewinnt man die oben gemeinte Formel

(21) $$\frac{t + u\sqrt{D}}{2} = \pm\left(\frac{\tau + v\sqrt{D}}{2}\right)^n,$$

um mittels der Fundamentalauflösung τ, v der *Pell*schen Gleichung, d. i. ihrer Auflösung in den kleinsten positiven Zahlen, sämtliche Auflösungen zu finden. Man hat zu diesem Zwecke nur in der Formel für jeden ganzzahligen Wert des Exponenten n und für jedes der beiden Vorzeichen die rechte Seite nach den Potenzen von $\sqrt{D}$ zu entwickeln, sodann den rationalen Bestandteil gleich $\frac{t}{2}$, den gesamten Koeffizienten von $\sqrt{D}$ gleich $\frac{u}{2}$ zu setzen und daraus t, u selbst zu ermitteln.

6. Die Kenntnis aller Auflösungen der *Pell*schen Gleichung gestattet uns nun, einige Aufgaben der Lehre von den quadratischen Formen, die wir noch unerledigt gelassen, zu lösen.

Ist $\varepsilon = \frac{t + u\sqrt{D}}{2}$ irgend eine Einheit und j ein Ideal des Körpers $\mathfrak{K}$, so ist stets $\varepsilon \cdot j = j$; denn, bezeichnet ζ irgend eine Zahl in j, so ist das in $\varepsilon \cdot j$ enthaltene Produkt $\varepsilon\zeta$ der Bedeutung eines Ideals zufolge auch in j enthalten, umgekehrt ist aber, da auch $\varepsilon'\zeta$ zu j gehört, jede Zahl $\zeta = 1 \cdot \zeta = \varepsilon \cdot \varepsilon'\zeta$ des Ideals j auch eine Zahl des Ideals $\varepsilon \cdot j$, und somit stimmen die Zahlen in j und in $\varepsilon \cdot j$ überein. Setzt man nun j in der Form (49) vorigen Kapitels und

$$\zeta = sa \cdot x - \frac{-b + \sqrt{D}}{2} \cdot sy$$

voraus, so ist (nach Nr. 10 daselbst)

$$(22)\quad N(\zeta) = s^2 a(ax^2 + bxy + cy^2) = s^2\left(\left(ax + \frac{by}{2}\right)^2 - \frac{Dy^2}{4}\right)$$

mithin, da $N(\varepsilon\zeta) = N(\varepsilon)\cdot N(\zeta)$ ist,

$$(23)\qquad N(\varepsilon\zeta) = s^2\left[\left(ax + \frac{by}{2}\right)^2 - \frac{Dy^2}{4}\right]\cdot\left(\frac{t^2 - Du^2}{4}\right).$$

Hier beachte man folgende Identität:

$$(24)\quad (t^2 - Du^2)\cdot(t'^2 - Du'^2) = (tt' + Duu')^2 - D(tu' + t'u)^2,$$

die nur ein ganz spezieller Fall der Identität (7) in Kap. 5 des 1. Abschnitts ist. Ihr zufolge läßt sich die Formel (23) schreiben wie folgt:

$$(25)\qquad \begin{cases} N(\varepsilon\zeta) = s^2\left(\left(aX + \frac{bY}{2}\right)^2 - D\cdot\frac{Y^2}{4}\right) \\ \qquad\qquad = s^2 a(aX^2 + bXY + cY^2), \end{cases}$$

wenn

$$(26)\quad X = \frac{t - bu}{2}\cdot x - cu\cdot y, \qquad Y = au\cdot x + \frac{t + bu}{2}\cdot y$$

gesetzt wird. Man sieht hieraus, daß der Multiplikation einer Zahl ζ des Ideals j mit einer Einheit $\varepsilon = \frac{t + u\sqrt{D}}{2}$ eine Transformation der dem Ideale zugeordneten Form (a, b, c) in sich selbst mittels der Gleichungen (26) entspricht, und es ist nicht schwer, auf Grund der voraufgehenden Untersuchungen nachzuweisen, daß diese Gleichungen (26) die sämtlichen sogenannten automorphen Transformationen der Form (a, b, c), d. i. diejenigen, durch welche sie in sich selbst übergeht, darstellen, wenn man nur solche ins Auge faßt, deren Determinante $+1$ ist.

Ist nämlich

$$(27)\qquad x = \lambda x' + \mu y', \qquad y = \nu x' + \varrho y'$$

eine Transformation T der Form (a, b, c), deren Determinante $+1$ ist, in die Form (a_1, b_1, c_1), so geht, wie wir wissen, die Wurzel ω der ersten Form in die gleichnamige Wurzel ω_1 der zweiten durch die Substitution

$$\omega = \frac{\lambda\omega_1 + \mu}{\nu\omega_1 + \varrho}$$

über, und umgekehrt folgt aus dieser Substitution jene Transformation. Mit der Identität beider Formen ist die ihrer Wurzeln gleichbedeutend. Demnach wird man alle jene automorphen Transformationen von (a, b, c) finden, wenn man alle Systeme $\lambda, \mu, \nu, \varrho$ ganzer, der Bedingung $\lambda\varrho-\mu\nu=1$ genügender Zahlen ermittelt, für welche

$$\omega = \frac{\lambda\omega + \mu}{\nu\omega + \varrho}$$

ist. Wie in Nr. 3 finden sich hierfür

$$\nu = au, \quad \varrho - \lambda = bu, \quad \mu = -cu,$$

und wenn man noch $\varrho + \lambda = t$ setzt, die Gleichungen

$$\lambda = \frac{t-bu}{2}, \quad \mu = -cu, \quad \nu = au, \quad \varrho = \frac{t+bu}{2},$$

wobei t, u durch die Gleichung $t^2 - Du^2 = 4$ bestimmt werden. Die automorphe Transformation (27) nimmt also die Form an:

$$(28) \quad x = \frac{t-bu}{2}\cdot x' - cu\cdot y', \quad y = au\cdot x' + \frac{t+bu}{2}\cdot y'$$

und stimmt so in der Tat mit der Transformation (26) bis auf die verschiedene Bezeichnung der Unbestimmten überein.

Nunmehr können auch alle Transformationen einer Form (a, b, c) in eine ihr äquivalente Form angegeben werden, sobald man eine derselben als bekannt voraussetzt. Die Feststellung der Äquivalenz selbst ergibt diese eine — wir bezeichnen sie als die Transformation (27) — aus ihr aber gehen alle hervor, wenn man sie mit allen Transformationen von (a, b, c) in sich selbst zusammensetzt. Bedeutet nämlich T eine solche, so geht offenbar (a, b, c) durch die sukzessive Anwendung der Transformationen T und T erst in sich selbst und dann in (a_1, b_1, c_1) über, und somit ist auch die zusammengesetzte Transformation $\mathrm{T}\cdot T$ eine der gesuchten. Ist umgekehrt außer T auch T_1 eine Transformation von (a, b, c) in (a_1, b_1, c_1), so stellt die Umkehrung von T eine Transformation T' von (a_1, b_1, c_1) in (a, b, c) vor, und die zusammengesetzte Transformation $\mathrm{T} = T_1 \cdot T'$ führt (a, b, c) in sich selbst über, stellt also eine automorphe Transformation dieser Form vor, die nun ihrerseits mit T zusammengesetzt

die Transformation $\mathrm{T} \cdot T = T_1 \cdot T' T$, d. i. die Transformation T_1 von (a, b, c) in (a_1, b_1, c_1), ergibt. Aus dieser Betrachtung folgt der **Satz:**

Aus der einen Transformation (27) der Form (a, b, c) in eine ihr äquivalente Form findet man sie sämtlich, soweit ihre Determinante $+1$ ist, mittels der Formeln:

$$(29) \qquad \begin{cases} X = \left(\frac{t - b u}{2} \lambda - c u \nu\right) x' + \left(\frac{t - b u}{2} \mu - c u \varrho\right) y', \\ Y = \left(a u \lambda + \frac{t + b u}{2} \nu\right) x' + \left(a u \mu + \frac{t + b u}{2} \varrho\right) y', \end{cases}$$

wenn darin für t, u alle ganzzahligen Auflösungen der *Pell*schen Gleichung gesetzt werden.

7. Wir kehren nun zu der Aufgabe zurück, alle eigentlichen Darstellungen zu finden, welche eine ganze Zahl m durch die Formen mit der Diskriminante D zuläßt.

In Nr. 6 des 5. Kap. vorigen Abschnitts ist gezeigt worden, daß eine solche Darstellung durch die besondere Form (a, b, c) mit der Diskriminante D nur möglich ist, wenn diese Form mit einer der Formen

$$(30) \qquad \left(m, r, \frac{r^2 - D}{4 m}\right),$$

in denen r jede der verschiedenen Wurzeln der Kongruenz

$$(31) \qquad z^2 \equiv D \pmod{4 m}$$

bedeutet, eigentlich äquivalent ist, da jede eigentliche Darstellung α, γ von m durch (a, b, c) zu einer bestimmten Wurzel r dieser Kongruenz gehört und eine Transformation von (a, b, c) mit der Determinante $+1$ in die entsprechende Form (30) ergibt, daß aber auch umgekehrt aus jeder solchen Transformation

$$x = \alpha x' + \beta y', \qquad y = \gamma x' + \delta y'$$

eine zur Wurzel r gehörige Darstellung α, γ von m durch (a, b, c) erhalten wird. Um daher sämtliche vorhandenen eigentlichen Darstellungen von m durch (a, b, c) zu finden, stellt sich folgende Regel heraus:

Man denke sie sich, je nachdem sie zu den einzelnen Wurzeln der Kongruenz gehören können, in verschiedene Darstellungsgruppen verteilt. Um die etwa zur Wurzel r

gehörigen zu finden, versuche man, ob die Form (a, b, c) mit der Form $\left(m, r, \frac{r^2 - D}{4m}\right)$ äquivalent ist, oder nicht — was nach den in Kap. 5 vor. Abschn. entwickelten Methoden ausführbar ist —; im letzteren Falle gibt es keine zu dieser Gruppe gehörigen Darstellungen. Andernfalls findet sich eine Transformation (27) von (a, b, c) in die Form $\left(m, r, \frac{r^2 - D}{4m}\right)$ und daraus mittels der Formeln (29) alle diese Transformationen; indem man aus jeder derselben den ersten und dritten Koeffizienten herausnimmt, gewinnt man alle zur Kongruenzwurzel r gehörigen Darstellungen von m durch (a, b, c) mittels der Formeln

$$(32) \qquad \alpha = \frac{t - bu}{2}\lambda - cu\nu, \qquad \gamma = au\lambda + \frac{t + bu}{2}\nu,$$

wenn man darin für t, u alle ganzzahligen Lösungen der *Pell*schen Gleichung gesetzt denkt. Wird dies für jede der verschiedenen Kongruenzwurzeln r durchgeführt, so erhält man die sämtlichen Gruppen von Darstellungen, deren die Zahl m durch die Form (a, b, c) fähig ist. Da die Anzahl der Lösungen t, u der *Pell*schen Gleichung eine endliche oder unendlich große ist, je nachdem D negativ oder positiv ist, wird für eine überhaupt durch die Form (a, b, c) darstellbare Zahl je nach diesen beiden Fällen die Anzahl ihrer Darstellungen ebenfalls endlich bzw. unendlich groß sein.

Indem hierbei sukzessive für (a, b, c) jede der Formen gewählt wird, welche ein Repräsentantensystem für die Diskriminante D ausmachen, ergeben sich auf solche Weise alle eigentlichen Darstellungen, welche die Zahl m durch das Formensystem jener Diskriminante D verstattet, und aus ihnen können ihre Darstellungen durch jede andere Form mit derselben Diskriminante, wie a. a. O. bemerkt worden ist, mittels der Transformation hergeleitet werden, welche diese Form in den ihr äquivalenten Repräsentanten verwandelt.

Beispiel. Um die Theorie der Darstellung einer Zahl durch eine quadratische Form und andere der früher entwickelten Lehren zu erläutern, betrachten wir an dieser Stelle ausführlich ein Beispiel. Es handle sich um die Dar-

stellung der Zahl $m = 21$ durch eine gegebene Form mit der positiven Diskriminante $D = 37$.

Vor allem stellen wir ein Repräsentantensystem für die Formen mit dieser Diskriminante auf und suchen zu diesem Zwecke alle reduzierten Formen (a, b, c).

Für diejenigen mit positivem a liegt b (nach Abschn. I, Kap. 5, Nr. 19) zwischen 0 und $-\sqrt{37}$ und kann also nur einen der Werte

$$-1, \ -2, \ -3, \ -4, \ -5, \ -6$$

oder vielmehr, da es wegen

$$(1') \qquad b^2 - 4ac = 37$$

ungerade sein muß, nur einen der Werte -1, -3, -5 haben. Für $b = -1$ liegt $2a$ zwischen $-1 + \sqrt{37}$ und $1 + \sqrt{37}$, a kann also nur 3 sein, und dementsprechend ist wegen

$$(2') \qquad \frac{b^2 - 37}{4a} = c$$

$c = -3$; dies gibt die reduzierte Form

$$f_1 = (3, \ -1, \ -3) \, .$$

Für $b = -3$ findet sich $2a$ zwischen $-3 + \sqrt{37}$ und $3 + \sqrt{37}$, also a als eine der Zahlen 2, 3, 4, denen aber kein ganzzahliges c entspricht.

Für $b = -5$ liegt $2a$ zwischen $-5 + \sqrt{37}$ und $5 + \sqrt{37}$, also kann a nur einen der Werte 1, 2, 3, 4, 5 haben, aber nur den Werten $a = 1$, $a = 3$ gehören ganzzahlige Werte $c = -3$, $c = -1$ resp. zu; man findet also noch die beiden reduzierten Formen

$$f_2 = (1, \ -5, \ -3), \qquad f_3 = (3, \ -5, \ -1) \, .$$

Bei den reduzierten Formen mit negativem a liegt b zwischen 0 und $\sqrt{37}$, kann also nur einen der Werte 1, 3, 5 haben. Für $b = 1$ liegt dann $2a$ zwischen $1 - \sqrt{37}$ und $-1 - \sqrt{37}$, a also müßte -3 sein, wofür dann $c = 3$ wird, und die reduzierte Form

$$f_4 = (-3, \ 1, \ 3)$$

hervorgeht. Für $b = 3$ fände sich $2a$ zwischen $3 - \sqrt{37}$ und $-3 - \sqrt{37}$, also a gleich einem der Werte $-2, -3, -4$, denen aber wieder kein ganzzahliges c entspricht. Für $b = 5$ dagegen liegt $2a$ zwischen $5 - \sqrt{37}$ und $-5 - \sqrt{37}$, also hätte a einen der Werte $-1, -2, -3, -4, -5$, von denen aber nur $a = -1, -3$ ganzzahlige Werte $c = 3, 1$ resp. ergeben, also zu noch zwei weiteren reduzierten Formen

$$f_5 = (-1, 5, 3), \quad f_6 = (-3, 5, 1)$$

führen. Es gibt somit im ganzen sechs reduzierte Formen.

Ihre ersten Wurzeln sind

$$\omega_1 = \frac{1 + \sqrt{37}}{6}, \quad \omega_2 = \frac{5 + \sqrt{37}}{2}, \quad \omega_3 = \frac{5 + \sqrt{37}}{6},$$

$$\omega_4 = \frac{1 - \sqrt{37}}{6}, \quad \omega_5 = \frac{5 - \sqrt{37}}{2}, \quad \omega_6 = \frac{5 - \sqrt{37}}{6},$$

die zweiten Wurzeln der drei letzten Formen aber

$$\omega_4' = \frac{1 + \sqrt{37}}{6}, \quad \omega_5' = \frac{5 + \sqrt{37}}{2}, \quad \omega_6' = \frac{5 + \sqrt{37}}{6},$$

also mit den ersten Wurzeln der drei ersten Formen identisch, und somit gibt es nur die drei reduzierten Zahlen $\omega_1, \omega_2, \omega_3$ der Gesamtheit Ω. Nun ist aber

$$\omega_1 = \frac{1 + \sqrt{37}}{6} = 1 + \frac{\sqrt{37} - 5}{6} = 1 + \frac{12}{6(\sqrt{37} + 5)} = 1 + \frac{1}{\omega_2}$$

$$\omega_2 = \frac{5 + \sqrt{37}}{2} = 5 + \frac{\sqrt{37} - 5}{2} = 5 + \frac{12}{2(\sqrt{37} + 5)} = 5 + \frac{1}{\omega_3}$$

$$\omega_3 = \frac{5 + \sqrt{37}}{6} = 1 + \frac{\sqrt{37} - 1}{6} = 1 + \frac{36}{6(\sqrt{37} + 1)} = 1 + \frac{1}{\omega_1}.$$

Demnach erhält man die Kettenbruchentwicklungen

$$(3') \quad \begin{cases} \omega_1 = \lfloor 1, \omega_2 \rceil \\ \omega_1 = \lfloor 1, 5, \omega_3 \rceil \\ \omega_1 = \lfloor 1, 5, 1, \omega_1 \rceil \\ \omega_1 = \lfloor 1, 5, 1, 1, \omega_2 \rceil \\ \omega_1 = \lfloor 1, 5, 1, 1, 5, \omega_3 \rceil \\ \omega_1 = \lfloor 1, 5, 1, 1, 5, 1, \omega_1 \rceil \end{cases}$$

usw. Die Näherungsbrüche des letzten Kettenbruchs sind

$$\frac{1}{0}, \frac{1}{1}, \frac{6}{5}, \frac{7}{6}, \frac{13}{11}, \frac{72}{61}, \frac{85}{72}, \frac{85\,\omega_1 + 72}{72\,\omega_1 + 61}.$$

Hiernach gibt die zweite der Formeln (3′)

$$\omega_1 = \frac{6\,\omega_3 + 1}{5\,\omega_3 + 1}, \qquad 6 \cdot 1 - 1 \cdot 5 = 1,$$

die vierte derselben

$$\omega_1 = \frac{13\,\omega_2 + 7}{11\,\omega_2 + 6}, \qquad 13 \cdot 6 - 7 \cdot 11 = 1,$$

d. h. ω_2 und ω_3 sind eigentlich äquivalent mit ω_1, woraus nach Abschn. I, Kap. 5, Nr. 13 auch die eigentliche Äquivalenz der Formen f_1, f_2, f_3 hervorgeht. Ebenso erkennt man die eigentliche Äquivalenz der Formen f_4, f_5, f_6, da deren zweite Wurzeln mit ω_1, ω_2, ω_3 identisch sind.

Endlich geht aber auch f_4 aus f_1 hervor durch die Transformation

$$x = -y', \qquad y = x'$$

mit der Determinante $+1$, also sind auch f_1, f_4 und deshalb alle sechs reduzierte Formen miteinander eigentlich äquivalent.

Ist nun aber (a, b, c) irgend eine Form mit der Diskriminante 37 und hat sie eine positive Wurzel ω, so ist diese als eine positive Zahl der Gesamtheit Ω mit einer reduzierten Zahl derselben, d. i. mit einer der drei Zahlen ω_1, ω_2, ω_3 äquivalent, und da diese selbst äquivalent sind, so ist es ω mit ω_1, es besteht also eine Beziehung

$$\omega = \frac{\alpha\,\omega_1 + \beta}{\gamma\,\omega_1 + \delta}, \tag{4′}$$

worin $\alpha\delta - \beta\gamma = \pm 1$. Beachtet man aber die aus der dritten der Gleichungen (3′) hervorgehende Beziehung

$$\omega_1 = \frac{7\,\omega_1 + 6}{6\,\omega_1 + 5}, \qquad \text{mit} \qquad 7 \cdot 5 - 6 \cdot 6 = -1, \tag{5′}$$

welche, wenn dieser Wert von ω_1 in (4′) eingesetzt wird,

$$\omega = \frac{\alpha'\,\omega_1 + \beta'}{\gamma'\,\omega_1 + \delta'}$$

ergibt, so ist nun entsprechend

$$\alpha'\delta' - \beta'\gamma' = (\alpha\delta - \beta\gamma)\cdot(7\cdot 5 - 6\cdot 6) = \mp 1 .$$

Die Wurzel ω der Form (a, b, c) erweist sich also der ersten Wurzel ω_1 der Form f_1 sowohl eigentlich als uneigentlich äquivalent. Da nun

$$\omega_1' = \frac{1-\sqrt{37}}{6} = -\frac{\sqrt{37}-1}{6} = -\frac{36}{6(\sqrt{37}+1)} = -\frac{1}{\omega_1}$$

oder

$$\omega_1 = -\frac{1}{\omega_1'} = \frac{0\cdot\omega_1' - 1}{1\cdot\omega_1' + 0},$$

also ω_1 mit ω_1' eigentlich äquivalent ist, so sieht man, daß ω auch der andern Wurzel ω_1' der Form f_1 sowohl eigentlich als uneigentlich äquivalent ist. Aus der eigentlichen Äquivalenz der gleichnamigen Wurzeln zweier Formen ergab sich nach der angeführten Stelle die eigentliche Äquivalenz der Formen, und genau ebenso folgt aus der uneigentlichen Äquivalenz der ungleichnamigen Wurzeln die uneigentliche Äquivalenz der Formen. Hiernach ist (a, b, c) der Form f_1 sowohl eigentlich als auch uneigentlich äquivalent. Hätte (a, b, c) keine positive Wurzel, so gälte dies doch von der ihr uneigentlich äquivalenten, entgegengesetzten Form $(a, -b, c)$; da diese somit nach dem eben Bewiesenen mit f_1 eigentlich und uneigentlich äquivalent wäre, so ergäbe sich auch dann für die Form (a, b, c) das gleiche. Hieraus erkennt man schließlich, daß alle Formen mit der Diskriminante 37 nur eine einzige Klasse untereinander eigentlich wie uneigentlich äquivalenter Formen bilden, als deren Repräsentant die Form f_1 gewählt werden kann.

Ferner erschließt man aus der Beziehung (5'), indem man, den Formeln (13) dieses Kapitels entsprechend,

$$\frac{t+u}{2} = 7, \quad 3u = 6, \quad \frac{t-u}{2} = 5$$

setzt, in den Werten

$$t = 12, \quad u = 2$$

eine ganzzahlige Auflösung der Gleichung

$$t^2 - 37u^2 = -4 .$$

Aus der letzten der Gleichungen (3′) folgt die weitere Beziehung

$$\omega_1 = \frac{85\,\omega_1 + 72}{72\,\omega_1 + 61}$$

und, indem man jetzt

$$\frac{t+u}{2} = 85, \quad 3\,u = 72, \quad \frac{t-u}{2} = 61$$

setzt, findet man in den Werten

(6′) $$t = 146, \quad u = 24$$

die Fundamentalauflösung der *Pell*schen Gleichung

(7′) $$t^2 - 37\,u^2 = 4.$$

Demnach liefert die Formel

(8′) $$\frac{t + u\sqrt{37}}{2} = \pm(73 + 12 \cdot \sqrt{37})^n$$

alle Lösungen derselben, wenn n alle ganzzahligen Werte durchläuft. Ihr zufolge sind t, u stets gerade Zahlen, und daher

$$\tau = \frac{t}{2}, \quad v = \frac{u}{2}$$

die Auflösungen der Gleichung

$$x^2 - 37\,y^2 = 1,$$

deren Fundamentalauflösung also $x = 73$, $y = 12$ ist. Z. B. ergibt sich aus (8′) für $n = 3$ und für das obere Vorzeichen

$$\tau + v\sqrt{37} = (73 + 12\sqrt{37})^3 = 1555849 + 255780 \cdot \sqrt{37},$$

also

(9′) $$\tau = 1555849, \quad v = 255780$$

und man findet in der Tat

$$1555849^2 - 37 \cdot 255780^2 = 1. \text{ —}$$

Dies vorausgeschickt, suchen wir nun alle eigentlichen Darstellungen der Zahl $m = 21$ durch eine beliebige der Formen mit der Diskriminante 37, z. B. durch deren Hauptform

(10′) $$f = x^2 + x\,y - 9\,y^2.$$

Dazu ist zunächst festzustellen, ob solche Darstellung überhaupt möglich, d. h., ob die Kongruenz

(11') $$x^2 \equiv 37 \pmod{4m = 84}$$

auflösbar ist. Soll dies der Fall sein, so muß auch jede der drei Kongruenzen

(12') $$x^2 \equiv 37 \pmod{4}, \quad x^2 \equiv 37 \pmod{3}, \quad x^2 \equiv 37 \pmod{7}$$

auflösbar sein. Dies trifft hier zu und ihre Wurzeln sind resp.

(13') $$x \equiv \pm 1 \pmod{4}, \quad x \equiv \pm 1 \pmod{3}, \quad x \equiv \pm 3 \pmod{7};$$

in der Tat befriedigen diese Werte von x die betreffende der Kongruenzen (12'), und jede der letzteren hat nur zwei Wurzeln, die zweite und die dritte, da ihr Modul eine Primzahl ist, die erste, da jede ihrer Lösungen ungerade sein, also eine der beiden Formen $4n \pm 1$ haben muß. Ist nun andererseits x eine Zahl, welche die drei Kongruenzen (12') gleichzeitig erfüllt, so ist $x^2 - 1$ teilbar durch jede der Zahlen 4, 3, 7, also auch durch ihr Produkt, und demnach genügt dann x auch der Kongruenz (11'). Um also alle Wurzeln der letzteren zu finden, hat man alle (mod. 84) inkongruenten Zahlen x zu ermitteln, welche den Bedingungen

(14') $$x \equiv u \pmod{4}, \quad x \equiv v \pmod{3}, \quad x \equiv w \pmod{7}$$

gleichzeitig genügen, während u, v, w jede der acht Kombinationen bedeuten, welche die in bezug auf diese Moduln nach (13') für x zulässigen Reste gestatten. Nach Abschn. I, Kap. 2, Nr. 4 ist es möglich, für jede dieser Kombinationen den Bedingungen (14') zu genügen, und bilden die ihnen genügenden Zahlen x je eine einzige Restklasse (mod. 84); demnach hat die Kongruenz (11') acht Wurzeln. Um sie zu finden, d. h. eine den Bedingungen (14') genügende Zahl zu ermitteln, kann man folgendermaßen verfahren. Man bestimme zunächst die Hilfszahlen λ, μ, ν durch die Bedingungen

(15') $$\begin{cases} 3 \cdot 7 \lambda \equiv 1 \pmod{4}, \quad 7 \cdot 4 \mu \equiv 1 \pmod{3}, \\ 4 \cdot 3 \nu \equiv 1 \pmod{7}; \end{cases}$$

solche Zahlen sind z. B.

$$\lambda = 1, \quad \mu = 1, \quad \nu = 3;$$

dann leistet die Zahl

(16') $x \equiv 3 \cdot 7 \lambda u + 7 \cdot 4 \mu v + 4 \cdot 3 \nu w \pmod{84}$

den Kongruenzen (14') Genüge, wie unmittelbar erkannt wird, wenn man vorstehende Kongruenz, statt auf den Modul 84, auf seine Teiler 4, 3, 7 als Moduln bezieht und (15') beachtet. Setzt man demzufolge der Reihe nach

$u = +1$	-1	-1	$+1$	$+1$	-1	$+1$	-1
$v = +1$	-1	$+1$	-1	-1	$+1$	$+1$	-1
$w = +3$	-3	$+3$	-3	$+3$	-3	-3	$+3$,

so finden sich entsprechend die Wurzeln

(17') $-11,\ +11,\ +31,\ -31,\ +17,\ -17,\ +25,\ -25$

(mod. 84) der Kongruenz (11'), und daraus folgen acht Formen von der oben mit $\left(m,\, r,\, \frac{r^2 - D}{4m}\right)$ bezeichneten Art:

(18') $$\begin{cases} F_1 = (21,\ +11,\ 1), & F_2 = (21,\ -11,\ 1) \\ F_3 = (21,\ +31,\ 11), & F_4 = (21,\ -31,\ 11) \\ F_5 = (21,\ +17,\ 3), & F_6 = (21,\ -17,\ 3) \\ F_7 = (21,\ +25,\ 7), & F_8 = (21,\ -25,\ 7). \end{cases}$$

Dem zuvor Bewiesenen zufolge sind sie sämtlich mit f eigentlich (und uneigentlich) äquivalent, und es gibt also zu jeder der acht Kongruenzwurzeln eine zugehörige Gruppe von unendlich viel eigentlichen Darstellungen der Zahl 21 durch die Form f. Um aus jeder dieser Gruppen je eine Darstellung zu ermitteln, entwickle man die ersten Wurzeln

$$\Omega_2 = \frac{11 + \sqrt{37}}{42}$$

$$\Omega_4 = \frac{17 + \sqrt{37}}{42}$$

$$\Omega_6 = \frac{31 + \sqrt{37}}{42}$$

$$\Omega_8 = \frac{25 + \sqrt{37}}{42}$$

der Formen F_2, F_4, F_6, F_8 in ihre Kettenbrüche, bis man, was nach Abschn. I, Kap. 5, Nr. 18 notwendig geschieht, zum Schlußnenner ω_1 gelangt. Man findet so

$$\Omega_2 = \lfloor 0,\ 2,\ 2,\ 5,\ 1,\ \omega_1 \rceil = \frac{13\,\omega_1 + 11}{32\,\omega_1 + 27}$$

$$\Omega_4 = \lfloor 0,\ 1,\ 7,\ 1,\ \omega_1 \rceil = \frac{8\,\omega_1 + 7}{9\,\omega_1 + 8}$$

$$\Omega_6 = \lfloor 0,\ 1,\ 1,\ 4,\ 1,\ \omega_1 \rceil = \frac{6\,\omega_1 + 5}{11\,\omega_1 + 9}$$

$$\Omega_8 = \lfloor 0,\ 1,\ 2,\ \omega_1 \rceil = \frac{2\,\omega_1 + 1}{3\,\omega_1 + 1}.$$

Sind ferner

$$\Omega_1 = \frac{-11 + \sqrt{37}}{42}$$

$$\Omega_3 = \frac{-31 + \sqrt{37}}{42}$$

$$\Omega_5 = \frac{-17 + \sqrt{37}}{42}$$

$$\Omega_7 = \frac{-25 + \sqrt{37}}{42}$$

die ersten Wurzeln der Formen F_1, F_3, F_5, F_7, so ist

$$\Omega_1 = -\frac{11 - \sqrt{37}}{42} = -\Omega_2',$$

wenn Ω_2' die zweite Wurzel von F_2 bezeichnet, woraus offenbar sich

$$\Omega_1 = -\frac{13\,\omega_1' + 11}{32\,\omega_1' + 27}$$

oder wegen $\omega_1' = -\dfrac{1}{\omega_1}$ sich

$$\Omega_1 = \frac{-11\,\omega_1 + 13}{27\,\omega_1 - 32}$$

ergibt; ebenso findet man

$$\Omega_3 = \frac{-7\,\omega_1 + 8}{8\,\omega_1 - 9}$$

$$\Omega_5 = \frac{-5\,\omega_1 + 6}{9\,\omega_1 - 11}$$

$$\Omega_7 = \frac{-\omega_1 + 2}{\omega_1 - 3}.$$

Aus diesen Gleichungen fließen umgekehrt die folgenden:

$$
(19') \quad \begin{cases}
\omega_1 = \dfrac{32\,\Omega_1 + 13}{27\,\Omega_1 + 11}, & 32\cdot 11 - 13\cdot 27 = 1 \\[2ex]
\omega_1 = \dfrac{-27\,\Omega_2 + 11}{32\,\Omega_2 - 13}, & 27\cdot 13 - 11\cdot 32 = -1 \\[2ex]
\omega_1 = \dfrac{9\,\Omega_3 + 8}{8\,\Omega_3 + 7}, & 9\cdot 7 - 8\cdot 8 = -1 \\[2ex]
\omega_1 = \dfrac{-8\,\Omega_4 + 7}{9\,\Omega_4 - 8}, & 8\cdot 8 - 7\cdot 9 = 1 \\[2ex]
\omega_1 = \dfrac{11\,\Omega_5 + 6}{9\,\Omega_5 + 5}, & 11\cdot 5 - 6\cdot 9 = 1 \\[2ex]
\omega_1 = \dfrac{-9\,\Omega_6 + 5}{11\,\Omega_6 - 6}, & 9\cdot 6 - 5\cdot 11 = -1 \\[2ex]
\omega_1 = \dfrac{3\,\Omega_7 + 2}{\Omega_7 + 1}, & 3\cdot 1 - 2\cdot 1 = 1 \\[2ex]
\omega_1 = \dfrac{-\Omega_8 + 1}{3\,\Omega_8 - 2}, & 1\cdot 2 - 1\cdot 3 = -1 .
\end{cases}
$$

Andererseits ist die Kettenbruchentwicklung der ersten Wurzel

$$\omega = \frac{-1 + \sqrt{37}}{2}$$

der Hauptform f diese:

$$\omega = \lfloor 2,\ 1,\ \omega_1 \rceil$$

oder auch

$$\omega = \lfloor 2,\ 1,\ 1,\ 5,\ 1,\ \omega_1 \rceil,$$

woraus sich sowohl

$$(20') \qquad \omega = \frac{3\,\omega_1 + 2}{\omega_1 + 1}, \quad 3\cdot 1 - 2\cdot 1 = 1$$

als auch

$$(21') \qquad \omega = \frac{33\,\omega_1 + 28}{13\,\omega_1 + 11}, \quad 33\cdot 11 - 28\cdot 13 = -1$$

ergibt. Verbindet man also die Formel (20′) mit der ersten, vierten, fünften und siebenten, dagegen die Formel (21′)

mit den übrigen der Formeln (19′), so gelangt man zu den Gleichungen

$$\omega = \frac{150\,\Omega_1 + 61}{59\,\Omega_1 + 24}, \qquad 150 \cdot 24 - 61 \cdot 59 = 1$$

$$\omega = \frac{5\,\Omega_2 - 1}{\Omega_2 + 0}, \qquad 5 \cdot 0 + 1 \cdot 1 = 1$$

$$\omega = \frac{521\,\Omega_3 + 460}{205\,\Omega_3 + 181}, \qquad 521 \cdot 181 - 460 \cdot 205 = 1$$

$$\omega = \frac{-6\,\Omega_4 + 5}{\Omega_4 - 1}, \qquad 6 \cdot 1 - 5 \cdot 1 = 1$$

$$\omega = \frac{51\,\Omega_5 + 28}{20\,\Omega_5 + 11}, \qquad 51 \cdot 11 - 28 \cdot 20 = 1$$

$$\omega = \frac{11\,\Omega_6 - 3}{4\,\Omega_6 - 1}, \qquad -11 \cdot 1 + 3 \cdot 4 = 1$$

$$\omega = \frac{11\,\Omega_7 + 8}{4\,\Omega_7 + 3}, \qquad 11 \cdot 3 - 8 \cdot 4 = 1$$

$$\omega = \frac{51\,\Omega_8 - 23}{20\,\Omega_8 - 9}, \qquad -51 \cdot 9 + 23 \cdot 20 = 1,$$

denen zufolge

f übergeht	durch die Transformation	
in F_1	$x = 150\,x' + 61\,y'$,	$y = 59\,x' + 24\,y'$
in F_2	$x = 5\,x' - y'$,	$y = x'$
in F_3	$x = 521\,x' + 460\,y'$,	$y = 205\,x' + 181\,y'$
in F_4	$x = -6\,x' + 5\,y'$,	$y = x' - y'$
in F_5	$x = 51\,x' + 28\,y'$,	$y = 20\,x' + 11\,y'$
in F_6	$x = 11\,x' - 3\,y'$,	$y = 4\,x' - y'$
in F_7	$x = 11\,x' + 8\,y'$,	$y = 4\,x' + 3\,y'$
in F_8	$x = 51\,x' - 23\,y'$,	$y = 20\,x' - 9\,y'$.

Hiernach liefern die Werte

150, 59; 5, 1; 521, 205; −6, 1; 51, 20; 11, 4; 11, 4; 51, 20;

$r \equiv 11, \; -11, \quad 31, \quad -31, \quad 17, \quad -17, \quad 25, \quad -25$

(mod. 84)

je eine Darstellung der Zahl 21 durch die Form f aus der durch die beigefügte Kongruenzwurzel bezeichneten Darstellungsgruppe. Diese Gruppen selbst werden dann erhalten, wenn in den Formeln

$$\alpha = \frac{t-u}{2}\lambda + 9u\nu\,, \qquad \gamma = u\lambda + \frac{t+u}{2}\nu\,,$$

welche die Formeln (32) dieses Kapitels für den hier vorliegenden Fall $a = 1$, $b = 1$, $c = -9$ sind, für λ, ν die bzw. angegebenen Werte, für t, u aber alle durch die Gleichung (8′) gegebenen Auflösungen der *Pell*schen Gleichung gesetzt werden. Z. B. geben die Formeln

$$\alpha = 5\cdot\frac{t-u}{2} + 9u\,, \qquad \gamma = 5u + \frac{t+u}{2}$$

die zur Wurzel -11 gehörige Gruppe; für $t = 2$, $u = 0$ liefern sie die Darstellung 5, 1 obiger Tabelle; setzt man für t, u die Fundamentalauflösung 146, 24, so findet man die Darstellung 521, 205. Ebenso liefern die Formeln

$$\alpha = -6\cdot\frac{t-u}{2} + 9u\,, \qquad \gamma = -6u + \frac{t+u}{2}$$

die zur Wurzel -31 gehörige Gruppe, und z. B. für $t = -146$, $u = -24$ die Darstellung 150, 59. Hieraus, wie auch schon aus der obigen Tabelle, ersieht man, daß ein und dieselbe Darstellung α, γ als zu zwei verschiedenen Wurzeln gehörig angesehen werden muß je nach der Wahl der Zahlen β, δ in der Gleichung

$$\alpha\delta - \beta\gamma = 1\,.$$

In der Tat ist in Nr. 4 des 5. Kap. des Abschn. I gezeigt worden, daß zwar, wenn β, γ durch eine andere Lösung

$$\beta' = \beta + \alpha z\,, \qquad \delta' = \delta + \gamma z$$

jener Gleichung ersetzt werden, der Ausdruck

$$r = (2a\alpha + b\gamma)\beta + (b\alpha + 2c\gamma)\delta\,,$$

welcher die der Darstellung α, γ der Zahl m zugehörige Wurzel angibt, (mod. $4m$) unverändert bleibt, so oft z eine gerade Zahl ist; für ungerade z dagegen entsteht ein Wert ϱ, welcher mit r nur (mod. $2m$) kongruent ist, und in der Tat

sind in der obigen Tabelle die Zahlenpaare 11, -31; -11, 31; 17, -25; -17, 25, denen die gleiche Darstellung zukam, je zwei (mod. 42) kongruente Zahlen. Die obigen acht Darstellungsgruppen stimmmen infolge davon paarweise überein und reduzieren sich auf nur vier verschiedene, welche etwa durch die Darstellungen

$$5, 1; \; -6, 1; \; 11, 4; \; 51, 20$$

repräsentiert werden können.

Drittes Kapitel.

Die Teilbarkeit im quadratischen Körper.

1. Nach Ermittlung aller Einheiten des Körpers $\mathfrak{K}$ handelt es sich nun um die genauere Untersuchung der Zerlegung seiner Zahlen in einfachste Faktoren, wie sie der Zerlegung der rationalen ganzen Zahlen in Primfaktoren entspricht. In Nr. 1 des vorigen Kapitels ist in dieser Hinsicht bereits festgestellt, daß jede ganze Zahl ζ des Körpers nur in eine endliche Anzahl (von Einheiten verschiedener) Faktoren zerlegt werden kann. Diesem Analogon mit der Theorie des rationalen Zahlenkörpers tritt nun aber ein fundamentaler Unterschied zwischen dieser und der Theorie des quadratischen Zahlenkörpers gegenüber: die Zerlegung der Zahl ζ in nicht weiter zerlegbare Faktoren ist hier im allgemeinen nicht, wie im rationalen Zahlenkörper, nur auf eine einzige Weise möglich, oder, was auf dasselbe hinauskommt: eine unzerlegbare Zahl ζ ermangelt im allgemeinen der für Primzahlen charakteristischen Eigenschaft, daß ein Produkt zweier Zahlen nur dann durch sie teilbar sein kann, wenn es einer seiner Faktoren ist. So ist, um ein von *Dedekind* gegebenes Beispiel anzuführen, im Körper $\mathfrak{K}(\sqrt{-5})$, dessen sämtliche ganzen Zahlen die Form $r + s\sqrt{-5}$ mit ganzzahligen r, s haben, die Zahl $-1 + 2\sqrt{-5}$, wie man sich leicht überzeugt, auf keine Weise in ganze Faktoren der angegebenen Form zerlegbar, man findet aber

$$N(-1 + 2\sqrt{-5}) = 21 = 3 \cdot 7\,,$$

und doch erweist sich keiner der (gleichfalls unzerlegbaren) Faktoren $3, 7$ teilbar durch $-1 + 2\sqrt{-5}$, und die Zahl 21

somit auf zwei wesentlich verschiedene Arten als Produkt von unzerlegbaren Faktoren dargestellt. Dies zeigt an, daß für die Teilbarkeit der ganzen Zahlen in $\mathfrak{K}$ die unzerlegbaren ganzen Zahlen des Körpers nicht die letzten Elemente, nicht die eigentlichen Grundfaktoren der Zerlegung ausmachen können. Um diese zu ermitteln, bedarf es einer anderen Auffassung der Teilbarkeit.

2. Man bemerke, daß, wenn eine ganze Zahl ζ des Körpers durch eine andere ξ teilbar, also $\zeta = \gamma \cdot \xi$ ist, wo auch γ eine Zahl des Moduls $\mathfrak{g}$ bedeutet, nicht nur ζ selbst, sondern mit ihr auch das gesamte Hauptideal $\mathfrak{g}\zeta$ im Hauptideal $\mathfrak{g}\xi$ enthalten ist, wie denn auch umgekehrt, wenn letzteres der Fall ist, auch die Zahl $\zeta = 1 \cdot \zeta$ selbst eine Zahl dieses Hauptideals, mithin von der Form $\zeta = \gamma \cdot \xi$, d. h. teilbar durch ξ ist. Hiernach kommt es ganz auf dasselbe hinaus, ob man sagt: ζ sei teilbar durch ξ, d. h. ξ ein Teiler von ζ, oder ob man sagt: das Hauptideal $\mathfrak{g}\zeta$ sei enthalten im Hauptideale $\mathfrak{g}\xi$. Obwohl dann also in Wahrheit $\mathfrak{g}\zeta$ nur einen Teil von $\mathfrak{g}\xi$ ausmacht, wollen wir doch, um den Ausdruck dem Verhältnisse zwischen der Zahl ζ und ihrem Teiler ξ anzupassen, das Ideal $\mathfrak{g}\xi$ einen Teiler des Ideals $\mathfrak{g}\zeta$ oder letzteres durch das erstere teilbar nennen. Überhaupt setzen wir **die Definition** fest:

Ein Ideal j heiße teilbar durch ein Ideal j' oder letzteres ein Teiler des ersten, wenn j in j' enthalten ist, d. h. wenn alle Zahlen des Ideals j auch Zahlen des Ideals j' sind.

Der Nutzen dieser Ausdrucksweise wird sich in Kürze herausstellen; er tritt schon darin zutage, daß wir den Satz, eine Zahl ζ sei teilbar durch ξ, durch den völlig gleichlautenden wie gleichbedeutenden: das Ideal $\mathfrak{g}\zeta$ sei teilbar durch $\mathfrak{g}\xi$, ersetzen dürfen.

Der gegebenen Definition zufolge ergibt sich weiter, daß, wenn ein Ideal j teilbar ist durch ein Ideal j', dies letztere aber teilbar durch ein Ideal j'', auch j durch j'' teilbar ist; denn, wenn die Zahlen von j zu denen von j', die letzteren aber zu den Zahlen von j'' rechnen, so gehören auch die ersteren den Zahlen von j'' an.

Das Ideal $\mathfrak{g}$ hat offenbar keinen Teiler außer sich selbst, denn es ist in keinem anderen enthalten. Jedes andere Ideal j hat jedenfalls den Teiler $\mathfrak{g}$ oder ist teilbar durch $\mathfrak{g}$, denn

alle seine Zahlen sind ganze Zahlen; desgleichen hat j den Teiler j, da es in sich selbst enthalten ist. Wir weisen zunächst nach, daß es nur eine endliche Anzahl von Teilern besitzt.

Hierzu wollen wir zeigen, daß eine gegebene rationale ganze Zahl m nur einer endlichen Anzahl von Idealen angehören kann. In der Tat, da jedes Ideal die Form $s \cdot [a, h + \theta]$ hat, so ist sa die kleinste rationale ganze Zahl, die es enthält, und jede andere darin enthaltene Zahl dieser Art ist ein Vielfaches von sa, denn unter allen Zahlen von der Form $sa \cdot x + s(h + \theta) \cdot y$ sind nur diejenigen rational, für welche $y = 0$, d. h. die Vielfachen von sa. Soll also m darin enthalten sein, so muß m solch ein Vielfaches oder sa ein Teiler von m sein. Demnach gehört m nur denjenigen Idealen an, für welche s, a eine Zerlegung eines Teilers d von m in zwei Faktoren darstellen, und da sowohl die Anzahl der Teiler d von m, als auch diejenige der Zerlegungen eines jeden von ihnen in zwei Faktoren nur eine endliche ist, so kann gewiß auch die Anzahl der Ideale, denen m angehört, nur eine endliche sein.

Dies vorausgeschickt, sei jetzt j ein gegebenes Ideal und j' irgend einer seiner Teiler. Dann muß, wie jede Zahl von j, so insbesondere auch die darin enthaltene kleinste rationale ganze Zahl dem Ideale j' angehörig sein; da sie aber nach dem eben Bewiesenen nur in einer endlichen Anzahl von Idealen enthalten sein kann, so kann auch die Anzahl verschiedener Teiler j' von j nur eine endliche sein.

3. Nun sei $j = j_1 \cdot j_2$ das Produkt zweier Ideale. Man sieht leicht ein, daß jeder der beiden Faktoren j_1, j_2 ein Teiler von j ist. Denn die Zahlen des Produkts entstehen bekanntlich, wenn die Zahlen in j_1 mit den Zahlen in j_2 multipliziert und solche Produkte nach Belieben zueinander addiert werden. Wenn aber die Zahlen von j_1 mit Zahlen von j_2, d. h. mit ganzen Zahlen multipliziert werden, so entstehen der Definition eines Ideals zufolge Zahlen in j_1, und Summen solcher Zahlen gehören, da das Ideal ein Modul ist, wieder zu j_1; demnach sind alle Zahlen des Produkts $j_1 \cdot j_2$ d. h. des Ideals j in j_1 enthalten oder j_1 ein Teiler von j, und ganz aus den gleichen Gründen ist j_2 ein Teiler von j.

Nun aber fragt es sich — und dieser Punkt ist der feste Punkt, auf dem die ganze Lehre von der Teil-

barkeit im Körper $\mathfrak{K}$ beruht — ob auch umgekehrt jeder Teiler eines Ideals j als ein Faktor desselben aufgefaßt werden, mit anderen Worten, ob, wenn das Ideal j durch ein Ideal j_1 teilbar ist, ein anderes Ideal j_2 so angegeben werden kann, daß $j = j_1 \cdot j_2$ wird. Wir zeigen leicht auf Grund des fundamentalen Satzes am Schlusse des ersten Kapitels, daß diese Frage zu bejahen ist.

Wenn nämlich j_1 ein Teiler von j, also j in j_1 enthalten ist, so ist für jedes Ideal j' offenbar auch das Produkt $j \cdot j'$ enthalten in $j_1 \cdot j'$. Nach dem angeführten Fundamentalsatze können wir aber das Ideal j' so wählen, daß das Produkt $j_1 \cdot j'$ ein Hauptideal $\mathfrak{g}\,\xi$ wird; somit werden dann auch alle Zahlen des Ideals $j \cdot j'$ Vielfache von ξ, d. i. von der Form $\gamma \cdot \xi$, wo γ eine ganze Zahl des Körpers bezeichnet. Die Gesamtheit j_2 dieser Zahlen γ bildet aber einen Modul, da, wenn $\gamma' \xi$ und $\gamma'' \xi$ zwei Zahlen in $j \cdot j'$ sind, auch ihre Summe und Differenz $(\gamma' \pm \gamma'')\xi$ Zahlen in $j \cdot j'$ und somit $\gamma' \pm \gamma''$ Zahlen der Gesamtheit j_2 sind. Sie ist aber zudem ein Ideal, denn, ist ζ irgend eine ganze Zahl des Körpers, so gehört mit $\gamma\xi$ zugleich auch $\zeta \cdot \gamma \xi = \zeta \gamma \cdot \xi$ dem Ideale $j \cdot j'$, und somit zugleich mit γ auch $\zeta\gamma$ der Gesamtheit j_2 an. Da man nun setzen darf $j \cdot j' = j_2 \cdot \xi$, so folgt weiter

$$j \cdot j_1 j' = j_1 j_2 \cdot \xi \quad \text{oder} \quad j \cdot \mathfrak{g}\,\xi = j_1 j_2 \cdot \xi,$$

d. h. wegen $\mathfrak{g} j = j$ einfacher $j \cdot \xi = j_1 j_2 \cdot \xi$, also auch $j = j_1 \cdot j_2$.

Man erkennt auf Grund dieser Überlegungen nunmehr die völlige Identität der beiden Begriffe „Teiler“ und „Faktor“ eines Ideals.

4. Da wir nun in Nr. 2 die Teilbarkeit einer Zahl ζ durch eine andere Zahl ξ durch die Teilbarkeit des Ideals $\mathfrak{g}\zeta$ durch das Ideal $\mathfrak{g}\,\xi$ ersetzt haben, werden wir naturgemäß zu der allgemeineren Frage nach der Teilbarkeit der Ideale überhaupt geführt. Wir werden sehen, daß diese von ganz mit denen, welche für die Teilbarkeit der rationalen ganzen Zahlen gelten, übereinstimmenden Gesetzen beherrscht wird, und werden auf diese Weise schließlich auch die Teilbarkeit der ganzen Zahlen des quadratischen Körpers auf die Teilbarkeitsgesetze des rationalen wieder zurückführen können. Wir beginnen diese Entwicklung mit der Einführung einiger einfachen Begriffe.

Sind j_1, j_2 zwei Ideale und bedeuten allgemein ζ_1, ζ_2

die in jedem derselben resp. enthaltenen Zahlen, so ist die Gesamtheit j der Zahlen $\zeta_1 + \zeta_2$ wieder ein Ideal. In der Tat ist sie zunächst ein Modul, denn, sind ζ_1', ζ_1'' zwei der Zahlen ζ_1 und ζ_2', ζ_2'' zwei der Zahlen ζ_2, so gehören $\zeta_1' \pm \zeta_1''$ und $\zeta_2' \pm \zeta_2''$ resp. den Idealen j_1 und j_2, und somit

$$(\zeta_1' \pm \zeta_1'') + (\zeta_2' \pm \zeta_2'') = (\zeta_1' + \zeta_2') \pm (\zeta_1'' + \zeta_2'')$$

der Gesamtheit j an, die sonach zugleich mit zwei ihrer Zahlen $\zeta_1' + \zeta_2'$, $\zeta_1'' + \zeta_2''$ auch deren Summe und Differenz enthält. Die Gesamtheit j ist aber zudem auch ein Ideal. Denn, ist γ irgend eine ganze Zahl des Körpers, so gehören mit ζ_1, ζ_2 auch $\gamma\zeta_1, \gamma\zeta_2$ den Idealen j_1, j_2 resp. und deshalb gehört zugleich mit $\zeta_1 + \zeta_2$ auch $\gamma\zeta_1 + \gamma\zeta_2 = \gamma(\zeta_1 + \zeta_2)$ der Gesamtheit j an, d. h. jede Zahl in j gibt mit irgend einer Zahl γ in $\mathfrak{g}$ multipliziert wieder eine Zahl in j und daher ist j ein Ideal. Da nun jeder Modul, also auch jedes Ideal die Null enthält, so finden sich unter den Zahlen $\zeta_1 + \zeta_2$ auch die Zahlen $\zeta_1 + 0$, d. i. alle Zahlen des Ideals j_1, sowie die Zahlen $0 + \zeta_2$, d. i. alle Zahlen des Ideals j_2, also sind j_1, j_2 beide enthalten in j oder teilbar durch j und das Ideal j ist ein gemeinsamer Teiler von j_1 und j_2. Bezeichnet ferner j' irgend ein Ideal, das gemeinsamer Teiler von j_1 und j_2 ist, in welchem nämlich alle Zahlen ζ_1 von j_1, wie alle Zahlen ζ_2 von j_2 enthalten sind, so enthält es auch alle Zahlen $\zeta_1 + \zeta_2$, d. h. das Ideal j; demnach ist j teilbar durch j', d. h. jeder gemeinsame Teiler von j_1 und j_2 ist ein Teiler des besonderen ihnen gemeinsamen Teilers j, welcher wegen dieser Analogie mit dem Verhalten der gemeinsamen Teiler zweier rationalen ganzen Zahlen der größte gemeinsame Teiler der beiden Ideale j_1, j_2 genannt werden soll, obwohl er tatsächlich von allen ihnen gemeinsamen Teilern den kleinsten Umfang an Zahlen hat. Nach der Bildungsweise der Zahlen dieses Ideals j aus den Zahlen von j_1 und j_2 schreiben wir

(1) $$j = j_1 + j_2 .$$

Ist der so definierte größte gemeinsame Teiler zweier Ideale j_1, j_2 gleich $\mathfrak{g}$, so werden die Ideale j_1, j_2 zwei relativ prime Ideale genannt; solche sind also charakterisiert durch die Gleichung

(2) $$j_1 + j_2 = \mathfrak{g} .$$

5. Dem größten gemeinsamen Teiler zweier Zahlen steht ihr kleinstes gemeinsames Vielfaches gegenüber. Auch hierfür gibt es ein Analogon in der Theorie der Ideale. Sei jetzt j die Gesamtheit der Zahlen, welche zwei gegebenen Idealen j_1, j_2 gemeinsam sind; solche gibt es abgesehen von der ihnen gewiß gemeinsamen Zahl Null, denn z. B., enthalten j_1, j_2 die kleinsten rationalen Zahlen $s_1 a_1, s_2 a_2$ resp., so enthalten sie beide die Zahl $s_1 a_1 \cdot s_2 a_2$ und alle deren Vielfachen. Diese Gesamtheit j bildet wieder ein Ideal; denn, sind ζ', ζ'' zwei Zahlen derselben, also zugleich in j_1 und in j_2 enthalten, so sind auch $\zeta' \pm \zeta''$ sowohl in j_1 wie in j_2 und daher auch in der Gesamtheit j enthaltene Zahlen; desgleichen gehört, wenn γ irgend eine Zahl in $\mathfrak{g}$ bedeutet, mit einer Zahl ζ auch das Produkt $\gamma\zeta$ gleichzeitig den Idealen j_1, j_2 an, d. h. jede zu j gehörige Zahl gibt mit irgend einer Zahl in $\mathfrak{g}$ multipliziert wieder eine zu j gehörige Zahl; mithin ist j ein Ideal. Da alle seine Zahlen sowohl in j_1 als in j_2 enthalten sind, d. h. da j sowohl durch j_1 als auch durch j_2 teilbar ist, darf j ein gemeinsames Vielfaches von j_1, j_2 genannt werden. Bezeichnet aber j' irgend ein gemeinsames Vielfaches von j_1, j_2, nämlich ein Ideal, dessen sämtliche Zahlen sowohl in j_1 wie in j_2 enthalten sind, so gehören diese ja zu den Zahlen der Gesamtheit j, d. h. j' ist teilbar durch j oder ein Vielfaches von j. Man findet also: Jedes gemeinsame Vielfache der beiden Ideale j_1, j_2 ist ein Vielfaches des besonderen ihnen gemeinsamen Vielfachen j, welches wegen dieser Analogie mit der rationalen Zahlentheorie als kleinstes gemeinsames Vielfaches von j_1, j_2 bezeichnet werden soll, obwohl es tatsächlich von allen ihnen gemeinsamen Vielfachen den größten Umfang an Zahlen aufweist.

6. Sind zwei Ideale j_1, j_2 relativ prim, so ist der größte gemeinsame Teiler von $j_1 \cdot j$ und j_2, wo auch j ein Ideal, gleich demjenigen von j und j_2. Nach der Voraussetzung ist nämlich $j_1 + j_2 = \mathfrak{g}$, also auch

$$(3) \qquad (j_1 + j_2) j = \mathfrak{g} j = j \, .$$

Um die Zahlen des linksstehenden Produkts zu erhalten, sind bekanntlich alle Zahlen ζ in j mit allen Zahlen $\zeta_1 + \zeta_2$ des Ideals $j_1 + j_2$ zu multiplizieren und die Summen solcher

Produkte zu bilden, so daß jede Zahl des Ideals $(j_1 + j_2)j$ mit Hilfe des Summenzeichens durch

$$\Sigma(\zeta_1 + \zeta_2)\cdot\zeta = \Sigma\zeta_1\zeta + \Sigma\zeta_2\zeta$$

darstellbar, d. h. eine Zahl des Ideals $j_1 j + j_2 j$ ist. Da aber umgekehrt jede Zahl des letzteren die Form

$$\Sigma\zeta_1\zeta' + \Sigma\zeta_2\zeta'' = \Sigma(\zeta_1 + 0)\zeta' + \Sigma(0 + \zeta_2)\zeta''$$

hat, unter ζ', ζ'' Zahlen in j verstanden, und hiernach auch eine Zahl des Ideals $(j_1 + j_2)j$ darstellt, so sind ersichtlich die Ideale $j_1 j + j_2 j$ und $(j_1 + j_2)j$ einander gleich, und die Gleichung (3) läßt sich schreiben:

$$j_1 j + j_2 j = j,$$

woraus dann offenbar weiter

$$j_1 j + j_2 j + j_2 = j + j_2$$

hervorgeht. Da nun das Produkt $j_2 j$, wie in Nr. 3 gezeigt, durch j_2 teilbar, nämlich in j_2 enthalten ist, so wird die Summe aus jeder Zahl in $j_2 j$ und jeder Zahl in j_2, d. i. jede Zahl der Summe $j_2 j + j_2$ ebenfalls nur eine Zahl in j_2 sein können, mithin $j_2 j + j_2$ enthalten sein in j_2, während doch auch jede Zahl in j_2 als Summe aus der in $j_2 j$ enthaltenen Null und einer Zahl in j_2, d. h. als eine Zahl in $j_2 j + j_2$ darstellbar oder in letzterem Ideale enthalten ist. Da hiernach die Ideale j_2 und $j_2 j + j_2$ sich gegenseitig enthalten, ist $j_2 = j_2 j + j_2$ und die obige Gleichung geht über in die folgende:

(4) $$j_1 j + j_2 = j + j_2,$$

welche in der Tat nichts anderes ist, als der Ausdruck des behaupteten Satzes.

Hieraus schließen wir sogleich den wichtigen weiteren Satz:

Sind nicht nur j_1 und j_2, sondern auch j und j_2 relativ prime Ideale, so sind auch die Ideale $j_1 j$ und j_2 relativ prim. Denn bei diesen Voraussetzungen besteht nicht nur die Gleichung $j_1 + j_2 = \mathfrak{g}$, sondern auch die Gleichung $j + j_2 = \mathfrak{g}$, daher nimmt die aus der ersteren erschlossene Gleichung (4) die Gestalt an:

(5) $$j_1 j + j_2 = \mathfrak{g}$$

und lehrt die Richtigkeit des Satzes.

7. In diesen Sätzen haben wir die Grundlage gewonnen, um nun die Zerlegbarkeit der Ideale in eindeutig bestimmte einfache Faktoren zu erweisen. Wir nennen analog mit der Theorie des rationalen Körpers ein von $\mathfrak{g}$ verschiedenes Ideal j ein Primideal, wenn es außer den ihm stets zukommenden Teilern $\mathfrak{g}$ und j keine anderen Teiler besitzt. Man ersieht daraus sogleich, daß irgend ein anderes Ideal j_1 entweder teilbar durch j oder relativ prim sein muß zu j, denn der größte gemeinsame Teiler der Ideale j und j_1 kann nur der eine oder der andere der beiden Teiler $\mathfrak{g}$ und j sein, welche j besitzt, in Zeichen:

$$\text{entweder} \quad j + j_1 = \mathfrak{g}, \quad \text{oder} \quad j + j_1 = j;$$

im ersteren Falle sind j, j_1 relativ prim, im zweiten ist jede Summe $\zeta + \zeta_1$ aus irgend einer Zahl in j und irgend einer Zahl in j_1, also auch die Zahl $0 + \zeta_1 = \zeta_1$, d. h. jede Zahl des Ideals j_1 in j enthalten oder j_1 teilbar durch j. Auch schließen offenbar diese beiden Fälle sich aus, da j von $\mathfrak{g}$ verschieden zu denken ist.

Daraus folgt weiter die wichtigste Eigenschaft jedes Primideals j, daß ein Produkt zweier Ideale j_1, j_2 nur dann durch j teilbar sein kann, wenn es einer der Faktoren ist, ein Satz, der dann sofort auf Produkte aus einer beliebigen Anzahl von Faktoren ausgedehnt werden kann. In der Tat, ist keins der Ideale j_1, j_2 teilbar durch das Primideal j, so sind sie nach dem eben Bewiesenen beide relativ prim zu j, und daher ist zufolge des letzten Satzes voriger Nummer auch ihr Produkt relativ prim zu j, d. h. $j_1 j_2 + j = \mathfrak{g}$, mithin $j_1 j_2$ nicht teilbar durch j, denn sonst wäre $\mathfrak{g} = j_1 j_2 + j$ in j enthalten, was nicht sein kann, da j von $\mathfrak{g}$ verschieden gedacht wird.

Das Ideal $\mathfrak{g}$ spielt in der Theorie der Ideale ersichtlich die Rolle der Einheit. In der Tat ist stets, wie wir schon wissen, $\mathfrak{g} j = j$; ferner ist jedes Ideal teilbar durch $\mathfrak{g}$, weil seine Zahlen sämtlich ganze Zahlen sind; deshalb ist der größte gemeinsame Teiler von $\mathfrak{g}$ und irgend einem Ideale j gleich $\mathfrak{g}$, in Zeichen: $j + \mathfrak{g} = \mathfrak{g}$, denn da jede Zahl ζ des Ideals j auch eine Zahl in $\mathfrak{g}$ ist, so ist auch $\zeta + \gamma$ zugleich mit γ eine Zahl in $\mathfrak{g}$ und umgekehrt jede Zahl γ in $\mathfrak{g}$ gleich $0 + \gamma$, d. i. eine Zahl in $j + \mathfrak{g}$.

Man sieht endlich auch leicht, daß aus jeder Gleichung

$$\mathfrak{j}\,\mathfrak{j}_1 = \mathfrak{j}_1$$

zwischen Idealen die Gleichheit $\mathfrak{j} = \mathfrak{g}$ hervorgeht; in der Tat, multipliziert man jene mit einem Ideale $\mathfrak{j}'$ von der Beschaffenheit, daß $\mathfrak{j}_1 \cdot \mathfrak{j}'$ ein Hauptideal $\mathfrak{g}\,\xi$ wird, so findet sich $\mathfrak{j} \cdot \mathfrak{g}\,\xi$ d. i. $\mathfrak{j}\,\xi = \mathfrak{g}\,\xi$ und hieraus ersichtlich auch $\mathfrak{j} = \mathfrak{g}$, wie behauptet.

Hiernach darf man bei jeder Zerlegung eines Ideals in Faktoren vom Faktor $\mathfrak{g}$ abstrahieren oder zwei Zerlegungen, die sich nur durch diesen Faktor unterscheiden, als miteinander identisch betrachten.

8. Wir beweisen nun den fundamentalen Satz, daß jedes Ideal auf eindeutig bestimmte Weise als ein Produkt aus einer endlichen Anzahl von Primidealfaktoren dargestellt werden kann.

Zunächst hat jedes Ideal $\mathfrak{j}$ einen Primidealfaktor. Entweder ist nämlich $\mathfrak{j}$ selbst ein Primideal, und dann wäre für dasselbe der obige Satz schon bewiesen, denn dann verstattet $\mathfrak{j}$, da es außer $\mathfrak{j}$ und $\mathfrak{g}$ keinen Teiler hat, nur die Darstellungen $\mathfrak{j} = \mathfrak{j}$ oder $\mathfrak{j} = \mathfrak{g} \cdot \mathfrak{j}$, deren letztere nicht wesentlich von der ersteren verschieden ist.

Oder $\mathfrak{j}$ hat einen von $\mathfrak{g}$ und $\mathfrak{j}$ verschiedenen Idealteiler $\mathfrak{j}'$; dann darf gesetzt werden $\mathfrak{j} = \mathfrak{j}' \cdot \mathfrak{j}_1$, wo auch $\mathfrak{j}_1$ ein Ideal ist. Wäre hier $\mathfrak{j}'$ noch kein Primideal, so hätte es wieder einen von $\mathfrak{g}$ und $\mathfrak{j}'$ verschiedenen Idealteiler $\mathfrak{j}''$, und man könnte setzen $\mathfrak{j} = \mathfrak{j}'' \cdot \mathfrak{j}_1 \mathfrak{j}_2$, wo auch $\mathfrak{j}_2$ wieder ein Ideal bezeichnet. Wäre auch $\mathfrak{j}''$ noch kein Primideal, so könnte man wieder einen neuen Teiler $\mathfrak{j}'''$ von $\mathfrak{j}''$ finden, könnte $\mathfrak{j} = \mathfrak{j}''' \cdot \mathfrak{j}_1 \mathfrak{j}_2 \mathfrak{j}_3$ setzen und so weiter fortfahren, aber nicht ohne Ende; denn die Ideale

$$\mathfrak{j}_1, \ \mathfrak{j}_1 \mathfrak{j}_2, \ \mathfrak{j}_1 \mathfrak{j}_2 \mathfrak{j}_3, \ \cdots, \tag{6}$$

auf welche man so geführt wird, sind nicht nur sämtlich Teiler des Ideals $\mathfrak{j}$, sondern auch untereinander verschieden, da z. B. aus einer Gleichung

$$\mathfrak{j}_1 \mathfrak{j}_2 = \mathfrak{j}_1 \mathfrak{j}_2 \cdot \mathfrak{j}_3 \mathfrak{j}_4 \mathfrak{j}_5$$

nach dem in voriger Nummer Bemerkten sich

$$\mathfrak{g} = \mathfrak{j}_3 \mathfrak{j}_4 \mathfrak{j}_5$$

ergäbe, wonach $\mathfrak{g}$ durch ein Ideal j_8 teilbar, d. i. in j_8 enthalten wäre, was nur sein kann, wenn $j_8 = \mathfrak{g}$ wäre, gegen die Voraussetzung. Die Reihe der Ideale (6) würde also unendlich viel verschiedene Teiler von j ergeben, entgegen dem Umstande, daß ein Ideal nur eine endliche Anzahl von Teilern besitzt, wenn man nicht bei Fortsetzung des oben bezeichneten Prozesses einmal auf einen Primidealteiler von j geführt würde, den wir $\mathfrak{p}$ nennen wollen, und so der Prozeß endete. Demnach darf dann gesetzt werden

$$j = \mathfrak{p} \cdot j',$$

wo nun wieder j' ein Ideal bezeichnet.

Auf das letztere aber kann die gleiche Betrachtung in Anwendung gebracht, also $j' = \mathfrak{p}' \cdot j''$ gesetzt werden, wo $\mathfrak{p}'$ ein Primideal und auch j'' ein Ideal bezeichnet, dessen ersteres übrigens von $\mathfrak{p}$ nicht verschieden zu sein braucht. So kann man weiter fortfahren und erhält dann $j'' = \mathfrak{p}'' \cdot j'''$ usw., doch aus gleicher Erwägung wie vorher nicht ohne Ende, man muß vielmehr in der Reihe der Ideale $j', j'', j''', \ldots$ endlich einmal auf ein Ideal $j^{(i)}$ stoßen, welches selbst ein Primideal $\mathfrak{p}^{(i)}$ ist, somit den weiteren Fortgang schließt und die Formel

$$(7) \qquad j = \mathfrak{p} \cdot \mathfrak{p}' \cdot \mathfrak{p}'' \ldots \mathfrak{p}^{(i)},$$

d. i. die Zerlegung des Ideals j in lauter Primidealfaktoren ergibt.

Daß eine solche Zerlegung aber nur in eindeutiger Weise möglich ist, zeigt sich ganz ebenso wie bei der Zerlegung der rationalen ganzen Zahlen in Primfaktoren. Könnte man nämlich auch

$$j = \mathfrak{q} \cdot \mathfrak{q}' \cdot \mathfrak{q}'' \ldots \mathfrak{q}^{(k)}$$

setzen, wo auch $\mathfrak{q}, \mathfrak{q}', \ldots$ lauter Primideale bezeichnen, so müßte

$$(8) \qquad \mathfrak{p} \cdot \mathfrak{p}' \cdot \mathfrak{p}'' \ldots \mathfrak{p}^{(i)} = \mathfrak{q} \cdot \mathfrak{q}' \cdot \mathfrak{q}'' \ldots \mathfrak{q}^{(k)}$$

sein; das Ideal zur Linken hätte also das Primideal $\mathfrak{q}$ zum Teiler, was nur sein kann, wenn einer seiner Faktoren, etwa $\mathfrak{p}$, durch $\mathfrak{q}$ teilbar ist; aber $\mathfrak{p}$ hat als Primideal nur die Teiler $\mathfrak{p}$ und $\mathfrak{g}$, und da $\mathfrak{q}$ von $\mathfrak{g}$ verschieden ist, muß $\mathfrak{q} = \mathfrak{p}$ sein. Dann folgte aber durch Multiplikation von (8) mit

einem Ideale j_0, für welches $\mathfrak{p} j_0 = \mathfrak{q} j_0$ ein Hauptideal $\mathfrak{g} \xi$ wird, die Gleichung

$$\xi \cdot \mathfrak{g} \mathfrak{p}' \mathfrak{p}'' \ldots \mathfrak{p}^{(i)} = \xi \cdot \mathfrak{g} \mathfrak{q}' \mathfrak{q}'' \ldots \mathfrak{q}^{(k)},$$

also die einfachere Gleichung

$$\mathfrak{p}' \mathfrak{p}'' \ldots \mathfrak{p}^{(i)} = \mathfrak{q}' \mathfrak{q}'' \ldots \mathfrak{q}^{(k)},$$

die ebenso behandelt werden kann wie (8), und dann etwa die Gleichheit $\mathfrak{q}' = \mathfrak{p}'$ ergibt usw. Auf diese Weise zeigt sich die vollständige Übereinstimmung der einzelnen Primidealfaktoren beider Zerlegungen und daß ihre Anzahl hüben und drüben die gleiche sein muß.

Werden endlich die etwa gleichen Primidealfaktoren in der Zerlegung (7) zu Potenzen zusammengefaßt, so kann **der Fundamentalsatz** auch folgendermaßen ausgesprochen werden:

Jedes Ideal j kann auf eine eindeutig bestimmte Weise als Produkt aus Potenzen von Primidealfaktoren dargestellt werden nach der Formel

$$j = \mathfrak{p}^{a} \cdot \mathfrak{p}'^{a'} \ldots \mathfrak{p}^{(i) a^{(i)}}, \tag{9}$$

worin $a, a', \ldots a^{(i)}$ positive ganze Zahlen bezeichnen.

9. Die völlige Gleichmäßigkeit der Gesetze für die Teilbarkeit der Ideale und derjenigen für die Teilbarkeit der rationalen ganzen Zahlen, die sich in den letzten beiden Nummern ausgesprochen hat, erhält sich nun auch weiterhin durch die ganze Theorie hindurch. Es muß hier genügen, dies in einigen wichtigen Punkten festzustellen, welche die Theorie der Kongruenzen betreffen.

Schon in Nr. 7 des ersten Kapitels haben wir alle Zahlen der Gesamtheit $\mathfrak{g}$ in bezug auf einen darin enthaltenen Modul $\mathfrak{m}$ in Klassen kongruenter Zahlen verteilt und deren Anzahl als Norm von $\mathfrak{m}$ und durch das Symbol $\mathfrak{N}(\mathfrak{m})$ bezeichnet. Wählen wir jetzt für diesen Modul ein Primideal $\mathfrak{p}$ und setzen zur Abkürzung $\pi = \mathfrak{N}(\mathfrak{p})$; dann gibt es also π Zahlen $\zeta_0, \zeta_1, \zeta_2, \ldots, \zeta_{\pi-1}$ in $\mathfrak{g}$, welche (mod. $\mathfrak{p}$) untereinander inkongruent sind und für die Gesamtheit $\mathfrak{g}$ ein vollständiges Restsystem derart ausmachen, daß jede Zahl in $\mathfrak{g}$ einer und nur einer jener π Zahlen kongruent ist (mod. $\mathfrak{p}$); eine dieser Zahlen, etwa ζ_0, wird kongruent Null, d. h. in $\mathfrak{p}$ enthalten sein und kann geradezu gleich Null

vorausgesetzt werden, die übrigen sind im Ideale $\mathfrak{p}$ nicht enthalten.

Nach Einführung dieses allgemeineren Kongruenzbegriffs kann man nun wieder die Aufgabe stellen, eine gegebene Kongruenz aufzulösen. Sei

$$f(x) = \alpha_k x^k + \alpha_{k-1} x^{k-1} + \ldots + \alpha_1 x + \alpha_0$$

eine ganze Funktion von x, deren Koeffizienten ganze Zahlen des Körpers $\mathfrak{K}$ bezeichnen; wir setzen voraus, daß α_k nicht im Ideale $\mathfrak{p}$ enthalten sei, und nennen dann die Funktion vom Grade k. Dann gilt ganz analog mit Kap. 2 Nr. 2 des ersten Abschnittes der Satz:

Die Kongruenz

$$(10) \qquad f(x) \equiv 0 \pmod{\mathfrak{p}}$$

kann nicht mehr Wurzeln, d. h. (mod. $\mathfrak{p}$) inkongruente Lösungen haben, als ihr Grad beträgt. Dabei heißt „Lösung" ein Wert $x = \zeta$, der eine ganze Zahl des Körpers $\mathfrak{K}$ ist und so beschaffen, daß die Zahl

$$\alpha_k \zeta^k + \alpha_{k-1} \zeta^{k-1} + \ldots + \alpha_1 \zeta + \alpha_0$$

dem Ideale $\mathfrak{p}$ angehört. Der Beweis ist fast wörtlich der gleiche wie a. a. O. Zunächst überzeugt man sich leicht, daß der Satz für jede Kongruenz ersten Grades

$$\alpha_1 x + \alpha_0 \equiv 0 \pmod{\mathfrak{p}}$$

gilt. Hätte diese nämlich zwei inkongruente Lösungen ζ_1, ζ_2, so daß $\alpha_1 \zeta_1 + \alpha_0$, $\alpha_1 \zeta_2 + \alpha_0$ in $\mathfrak{p}$ vorhandene Zahlen wären, so wäre dies auch die Differenz $\alpha_1(\zeta_1 - \zeta_2)$ beider Zahlen, in welcher jedoch weder α_1 noch $\zeta_1 - \zeta_2$ in $\mathfrak{p}$ enthalten sind; dann kann aber auch jene Differenz keine Zahl in $\mathfrak{p}$ sein, denn sonst wäre zugleich mit ihr das ganze Hauptideal $\mathfrak{g} \cdot \alpha_1(\zeta_1 - \zeta_2)$ in $\mathfrak{p}$ enthalten; da aber $\mathfrak{g}$ ein Ideal und daher $\mathfrak{g}\mathfrak{g} = \mathfrak{g}$ ist, läßt sich dies Hauptideal schreiben wie folgt:

$$\mathfrak{g}\mathfrak{g} \cdot \alpha_1(\zeta_1 - \zeta_2),$$

was man, in Erinnerung an die Art und Weise, wie die Zahlen eines Idealprodukts aus den Zahlen seiner Idealfaktoren gebildet werden, sogleich als identisch erkennt mit $\mathfrak{g}\alpha_1 \cdot \mathfrak{g}(\zeta_1 - \zeta_2)$. Wenn aber dieses Produkt in $\mathfrak{p}$ enthalten oder durch das Primideal $\mathfrak{p}$ teilbar sein soll, so muß es auch einer seiner Faktoren sein, d. h. dieser Faktor $\mathfrak{g}\alpha_1$

oder $\mathfrak{g}(\zeta_1 - \zeta_2)$ und daher auch α_1 resp. $\zeta_1 - \zeta_2$ müßte in $\mathfrak{p}$ enthalten sein, gegen die Voraussetzungen.

Nachdem so der Satz für Kongruenzen ersten Grades als gültig befunden, nehmen wir nun an, er sei bereits für alle Kongruenzen geringeren als $k$ten Grades bewiesen, und zeigen, daß er dann auch für diejenigen $k$ten Grades besteht; so wird durch allgemeine Induktion dann seine Allgemeingültigkeit erwiesen sein. Zu diesem Zwecke nehme man an, die Kongruenz (10) habe im Gegenteil mindestens $k+1$ Wurzeln $\zeta_0, \zeta_1, \zeta_2, \ldots, \zeta_k$; dann hätte die Kongruenz höchstens $k-1$ten Grades

$$f(x) - \alpha_k(x-\zeta_1)(x-\zeta_2)\ldots(x-\zeta_k) \equiv 0 \pmod{\mathfrak{p}}$$

die k inkongruenten Lösungen $\zeta_1, \zeta_2, \ldots, \zeta_k$ und müßte dem vorausgesetzten Satze gemäß identisch, d. h. für jeden Wert von x, der eine ganze Zahl des Körpers $\mathfrak{K}$ ist, also auch für $x = \zeta_0$ erfüllt sein. Da aber nach Voraussetzung $f(\zeta_0) \equiv 0 \pmod{\mathfrak{p}}$, so ergäbe sich dann aus vorstehender Kongruenz die andere:

$$\alpha_k(\zeta_0-\zeta_1)(\zeta_0-\zeta_2)\ldots(\zeta_0-\zeta_k) \equiv 0 \pmod{\mathfrak{p}},$$

von der genau wie vorher bewiesen wird, daß sie nicht bestehen kann, da kein Faktor des Produkts in $\mathfrak{p}$ enthalten ist. Die Kongruenz (10) kann also nicht mehr als k Wurzeln haben, w. z. b. w.

10. Werden ferner die Glieder $\zeta_1, \zeta_2, \ldots, \zeta_{\pi-1}$ eines vollständigen Restsystems (mod. $\mathfrak{p}$) für die Gesamtheit $\mathfrak{g}$, welche nicht in $\mathfrak{p}$ enthalten sind, mit irgend einer ganzen Zahl ζ des Körpers, die ebenfalls nicht in $\mathfrak{p}$ enthalten ist, multipliziert, so entstehen $\pi - 1$ Produkte

$$\zeta\zeta_1, \zeta\zeta_2, \ldots, \zeta\zeta_{\pi-1}, \tag{11}$$

die, was geradeso wie in voriger Nummer gezeigt wird, auch nicht in $\mathfrak{p}$ enthalten sein können und zudem inkongruent sind (mod. $\mathfrak{p}$), da aus

$$\zeta\zeta_i \equiv \zeta\zeta_k \pmod{\mathfrak{p}}$$

sich $\zeta(\zeta_i - \zeta_k)$ als eine in $\mathfrak{p}$ enthaltene Zahl ergäbe, während doch weder ζ noch $\zeta_i - \zeta_k$ eine Zahl in $\mathfrak{p}$ ist. Hiernach bilden die Zahlen (11) wieder ein bis auf das eine in $\mathfrak{p}$ enthaltene Glied vollständiges Restsystem (mod. $\mathfrak{p}$) für die Gesamtheit $\mathfrak{g}$, und deshalb sind sie, von der Ordnung etwa

abgesehen, den Zahlen $\zeta_1, \zeta_2, \ldots, \zeta_{\pi-1}$ kongruent. Da man nun wieder, ganz analog wie bei den gewöhnlichen Kongruenzen zwischen ganzen rationalen Zahlen, auch für die hier betrachteten allgemeineren Kongruenzen einsieht, daß verschiedene Kongruenzen, die nach dem gleichen Modul stattfinden, miteinander addiert, subtrahiert oder multipliziert werden können, wie Gleichungen, so wird auch das Produkt der Zahlen (11) dem Produkte der Zahlen $\zeta_1, \zeta_2, \ldots, \zeta_{\pi-1}$ kongruent sein, also die Kongruenz

$$\zeta^{\pi-1} \cdot \zeta_1 \zeta_2 \ldots \zeta_{\pi-1} \equiv \zeta_1 \zeta_2 \ldots \zeta_{\pi-1} \pmod{\mathfrak{p}}$$

hervorgehen, aus welcher sich die Differenz beider Seiten:

$$(\zeta^{\pi-1} - 1) \cdot \zeta_1 \zeta_2 \ldots \zeta_{\pi-1}$$

als eine im Ideale $\mathfrak{p}$ enthaltene Zahl ergibt. Demnach folgert man wieder, daß das Produkt

$$\mathfrak{g}(\zeta^{\pi-1} - 1) \cdot \mathfrak{g}\, \zeta_1 \zeta_2 \ldots \zeta_{\pi-1}$$

durch das Primideal $\mathfrak{p}$ teilbar ist; der zweite Faktor kann es nicht sein, da sonst zugleich mit ihm insbesondere auch die Zahl $\zeta_1 \zeta_2 \ldots \zeta_{\pi-1}$ in $\mathfrak{p}$ enthalten sein müßte, während es doch keiner der Faktoren $\zeta_1, \zeta_2, \ldots, \zeta_{\pi-1}$ ist; mithin muß der erste Faktor durch $\mathfrak{p}$ teilbar, d. h. in $\mathfrak{p}$ enthalten und also auch $\zeta^{\pi-1} - 1$ eine Zahl des Ideals $\mathfrak{p}$ oder

$$\zeta^{\pi-1} \equiv 1 \pmod{\mathfrak{p}} \tag{12}$$

sein. Wir sind also durch ganz entsprechende Folgerungen, wie in Abschn. I, Kap. 2, Nr. 8, zu einem Satze gelangt, der als *Fermat*scher Satz im quadratischen Körper zu bezeichnen ist und folgendes aussagt:

Für jede in einem Primideal $\mathfrak{p}$ nicht enthaltene ganze Zahl ζ des Körpers besteht die Kongruenz (12) oder, wenn die Bedeutung von π beachtet wird, die Kongruenz

$$\zeta^{\mathfrak{N}(\mathfrak{p})-1} \equiv 1 \pmod{\mathfrak{p}}\,. \tag{13}$$

Nachdem durch diesen Satz für jede solche Zahl ζ eine Potenz nachgewiesen ist, welche (mod. $\mathfrak{p}$) der Eins kongruent ist, wird auch eine niedrigste Potenz dieser Art vorhanden sein. Ist ζ^e diese niedrigste der Eins (mod. $\mathfrak{p}$) kongruente Potenz von ζ, so mag wieder, wie in Nr. 9 des angegebenen Kapitels, e der Exponent heißen, zu welchem ζ (mod. $\mathfrak{p}$) gehört. Man überzeugt sich dann durch einfache Wieder-

holung ganz gleicher Schlüsse wie dort, daß e ein Teiler von $\mathfrak{N}(\mathfrak{p}) - 1$ sein muß, nicht minder davon, daß es in $\mathfrak{p}$ nicht enthaltene ganze Zahlen ζ des Körpers gibt, welche zu diesem größten aller Exponenten $\mathfrak{N}(\mathfrak{p}) - 1$ gehören und wieder als primitive Wurzeln (mod. $\mathfrak{p}$) bezeichnet werden mögen. Wir müssen jedoch die weiteren Ausführungen dieser Räsonnements dem Leser überlassen, wie wir auch darauf verzichten müssen, noch weiter die vollständige Analogie zu verfolgen, welche zwischen der Theorie der Ideale und derjenigen der rationalen ganzen Zahlen besteht.

11. Indem aber solcherweise die Arithmetik des Körpers $\mathfrak{K}$ auf seine Primideale als wesentliche Grundelemente aufgebaut wird, handelt es sich nun noch darum, diese letzteren zu ermitteln. Wir schicken solcher Untersuchung einen einfachen Hilfssatz voraus.

Ist j irgend ein Ideal und $i = \mathfrak{N}(j)$, so läßt sich die Gesamtheit $\mathfrak{g}$ in i Klassen (mod. j) kongruenter Zahlen verteilen; seien $\zeta_0, \zeta_1, \zeta_2, \ldots, \zeta_{i-1}$ ein vollständiges Restsystem für jene Gesamtheit; dann erhält man alle Zahlen in $\mathfrak{g}$ mittels der Formeln

$$(14) \qquad \zeta_0 + \eta, \quad \zeta_1 + \eta, \quad \zeta_2 + \eta, \quad \ldots, \quad \zeta_{i-1} + \eta,$$

wenn man darin für η sämtliche Zahlen des Ideals j eingesetzt denkt, und erhält so auch jede Zahl in $\mathfrak{g}$ nur einmal, da, wenn η', η'' Zahlen in j bedeuten, niemals

$$\zeta_{h'} + \eta' = \zeta_{h''} + \eta'', \qquad \text{also} \qquad \zeta_{h'} - \zeta_{h''} = \eta'' - \eta'$$

d. i. gleich einer in j enthaltenen Zahl sein kann, ohne daß gleichzeitig $h' = h''$ und $\eta' = \eta''$ ist. Wenn nun ein zweites Ideal j' durch j teilbar, d. i. in j enthalten ist, so lassen sich wieder auch alle Zahlen des Ideals j in bezug auf den Modul j' in Klassen kongruenter Zahlen verteilen, deren Anzahl k sei und durch (j, j') bezeichnet werde. Setzt man demgemäß $\eta_0, \eta_1, \eta_2, \ldots, \eta_{k-1}$ als ein vollständiges Restsystem (mod. j') für die Gesamtheit der Zahlen in j voraus, so daß alle Zahlen des Ideals j und wieder jede auch nur einmal durch die Formeln

$$\eta_0 + \xi, \quad \eta_1 + \xi, \quad \ldots, \quad \eta_{k-1} + \xi$$

erhalten werden, wenn man darin für ξ sämtliche Zahlen

des Ideals j' gesetzt denkt, so entstehen wegen (14) offenbar alle Zahlen in $\mathfrak{g}$ mittels der $i \cdot k$ Formeln

$$(15) \qquad \zeta_r + \eta_s + \xi \quad \text{für} \quad \begin{cases} r = 0, 1, 2, \ldots, i-1 \\ s = 0, 1, 2, \ldots, k-1, \end{cases}$$

wenn auch hier für ξ sämtliche Zahlen des Ideals j' eingesetzt werden.

Die $i \cdot k$ Zahlen $\zeta_r + \eta_s$ sind aber (mod. j') inkongruent; denn, wären zwei derselben kongruent, etwa

$$\zeta_r + \eta_s \equiv \zeta_{r'} + \eta_{s'} \quad (\text{mod.}\, j'),$$

d. h., wäre die Differenz

$$(16) \qquad (\zeta_r - \zeta_{r'}) + (\eta_s - \eta_{s'})$$

eine in j' enthaltene Zahl, so wäre sie auch enthalten in j, und da $\eta_s - \eta_{s'}$ zugleich mit $\eta_s, \eta_{s'}$ eine Zahl des Ideals j ist, so müßte auch $\zeta_r - \zeta_{r'}$ eine solche Zahl sein, was nach der Bedeutung der Zahlen $\zeta_r, \zeta_{r'}$ nur sein kann, wenn sie miteinander identisch sind. Da alsdann aber die Differenz (16) sich auf $\eta_s - \eta_{s'}$ reduziert, diese letztere Differenz also nach der Annahme in j' enthalten sein würde, müßten die Zahlen $\eta_s, \eta_{s'}$ ihrer Bedeutung zufolge miteinander identisch sein und somit gleiches gelten auch von den Zahlen $\zeta_r + \eta_s$, $\zeta_{r'} + \eta_{s'}$. Man erkennt aus diesen Gründen, daß die $i \cdot k$ Zahlen $\zeta_r + \eta_s$ ein vollständiges Restsystem (mod. j') für die Gesamtheit $\mathfrak{g}$ darstellen, und daß somit $i \cdot k = \mathfrak{N}(j')$ ist. Dies spricht sich aus in folgendem **Satze:**

Ist ein Ideal j' teilbar durch ein Ideal j, so ist auch die Norm von j' teilbar durch die Norm von j, und es besteht die Gleichung

$$(17) \qquad \mathfrak{N}(j') = \mathfrak{N}(j) \cdot (j, j'),$$

der auch die symmetrischere Form

$$(\mathfrak{g}, j') = (\mathfrak{g}, j) \cdot (j, j')$$

gegeben werden kann. Dieser Gleichung gemäß sind die Normen von j und j' dann und nur dann gleich, wenn $(j, j') = 1$, d. h. wenn alle Zahlen in j nur eine einzige Klasse (mod. j') bilden, somit kongruent sind mit der in j wie in j' enthaltenen Null, d. h. sämtlich in j' enthalten sind. Da aber j' teilbar durch j vorausgesetzt ist, so sind

auch umgekehrt alle Zahlen von j' Zahlen von j und somit dann beide Ideale identisch. Man darf demnach sagen:

Ist j ein echter, d. h. von j' selbst verschiedener Teiler von j', so ist auch $\mathfrak{N}(j)$ ein echter Teiler von $\mathfrak{N}(j')$.

12. Indem wir nun zur Aufsuchung aller Primideale des quadratischen Körpers übergehen, bemerken wir vor allen Dingen, daß die kleinste in einem Primideale $\mathfrak{p}$ enthaltene rationale ganze Zahl eine Primzahl sein muß. Denn, wäre sie eine zusammengesetzte Zahl $m \cdot n$, so wäre zugleich mit dieser auch das ganze Hauptideal $\mathfrak{g} \cdot mn$, welches auch $\mathfrak{g}\mathfrak{g} \cdot mn = \mathfrak{g}m \cdot \mathfrak{g}n$ geschrieben werden kann, in $\mathfrak{p}$ enthalten oder teilbar durch $\mathfrak{p}$, woraus dann folgen würde, daß wenigstens einer der beiden Faktoren, etwa $\mathfrak{g}m$, durch $\mathfrak{p}$ teilbar, mithin alle seine Zahlen, insbesondere die rationale ganze Zahl $m < m \cdot n$ in $\mathfrak{p}$ enthalten wäre, gegen die Annahme, daß mn die kleinste dieser Zahlen sei. Jedem Primideale $\mathfrak{p}$ entspricht also eine rationale Primzahl p als kleinste darin enthaltene rationale ganze Zahl, und sie ist eindeutig bestimmt, nämlich die einzige im Ideale $\mathfrak{p}$ vorhandene Primzahl, da ja alle sonst in ihm enthaltenen rationalen ganzen Zahlen Vielfache der kleinsten im Ideal vorhandenen sein müssen. Da nun jedes Ideal die Form (Kap. 1, Nr. 9) eines Moduls $s \cdot [a, h + \theta]$ hat, so muß, wenn die kleinste rationale ganze Zahl des Ideals eine Primzahl p, insbesondere also, wenn das Ideal ein Primideal sein soll, $sa = p$, also entweder $s = p$, $a = 1$ oder $s = 1$, $a = p$ sein. Im ersteren Falle ist das Ideal

$$p \cdot [1, h + \theta] = p \cdot [1, \theta] = \mathfrak{g}p,$$

im zweiten Falle

$$[p, h + \theta] = \left[p, \frac{-b + \sqrt{D}}{2}\right],$$

während b eine ganze Zahl ist, welche der Kongruenz

$$(18) \qquad b^2 \equiv D \pmod{4p}$$

genügt; solches Ideal existiert also nur dann, wenn die letztere Kongruenz möglich ist. Hiernach unterscheiden wir zwei Fälle:

Erstens: die Kongruenz (18) ist unmöglich oder D quadratischer Nichtrest von $4p$, was voraussetzt, daß D durch p nicht aufgeht, denn sonst wäre $b = p$ oder $b = 2p$

eine Lösung der Kongruenz, je nachdem $D \equiv 1$ oder $D \equiv 0$ (mod. 4). In diesem Falle gibt es nur ein Ideal, nämlich das Ideal $\mathfrak{g}p$, dessen kleinste rationale ganze Zahl p ist, und dieses Ideal ist ein Primideal. Denn, hätte $\mathfrak{g}p$ einen von sich selbst und von $\mathfrak{g}$ verschiedenen Idealteiler $\mathfrak{j}$, so daß $\mathfrak{g}p = \mathfrak{j} \cdot \mathfrak{j}'$ gesetzt werden könnte, so müßte $\mathfrak{g}p$, also auch die Zahl p im Teiler $\mathfrak{j}$ enthalten sein. Da aber p Primzahl ist, könnte die kleinste in $\mathfrak{j}$ vorhandene rationale ganze Zahl nur entweder 1 oder p sein, folglich wäre $\mathfrak{j}$ gegen die Voraussetzung entweder gleich $\mathfrak{g}$ oder gleich $\mathfrak{g}p$, dem einzigen Ideale, das die kleinste rationale ganze Zahl p enthält. — Die Norm dieses Primideals $\mathfrak{g}p$ ist [Kap. 1, Formel (58)]

$$\mathfrak{N}(\mathfrak{g}p) = N(p) = p^2; \tag{19}$$

demgemäß nennen wir $\mathfrak{g}p$ ein Primideal zweiten Grades.

Zweitens: die Kongruenz (18) ist möglich oder D quadratischer Rest von $4p$. In diesem Falle gibt es eine der Kongruenz (18) genügende Zahl b, also neben dem Ideale $\mathfrak{g}p$ auch noch ein Ideal

$$\left[p, \frac{-b+\sqrt{D}}{2}\right]$$

der gedachten Beschaffenheit. Ist aber b' irgend eine andere Zahl, für welche $b'^2 \equiv D$ (mod. $4p$) ist, so entspricht auch ihr ein solches Ideal

$$\left[p, \frac{-b'+\sqrt{D}}{2}\right]. \tag{20}$$

Nun findet man $b'^2 \equiv b^2$ (mod. $4p$) oder $(b'-b)\cdot(b'+b)$ teilbar durch $4p$; demnach ist wenigstens einer der beiden Faktoren durch p, beide zugleich aber durch 2 teilbar, da b, b' gleichartig mit D, also auch untereinander gleichartig sind; man schließt also, daß entweder $b'-b$ oder $b'+b$ ein Vielfaches von $2p$, etwa gleich $2p\beta$ ist. Die dem Ideale (20) entsprechende Linearform

$$px + \frac{-b'+\sqrt{D}}{2}\cdot y = p(x-\beta y) + \frac{\mp b+\sqrt{D}}{2}y$$

stimmt also mit einer der beiden Formen

$$pu + \frac{-b+\sqrt{D}}{2}v, \quad pu + \frac{-b-\sqrt{D}}{2}v$$

überein, wenn man $x-\beta y=u$, $y=\pm v$ setzt, d. h. das Ideal (20) ist mit einem der beiden:

$$(21)\qquad \left[p, \frac{-b+\sqrt{D}}{2}\right], \quad \left[p, \frac{-b-\sqrt{D}}{2}\right],$$

die einander konjugiert sind, identisch. In diesem zweiten Falle gibt es also nur drei Ideale, deren kleinste rationale ganze Zahl p ist, nämlich außer dem Ideale $\mathfrak{g}p$ die beiden Ideale (21). Möglicherweise sind aber die beiden letzteren noch identisch. Um zu erkennen, wann dies etwa der Fall ist, untersuchen wir allgemeiner, wann eins von ihnen durch das andere teilbar oder in ihm enthalten ist. Soll das erste im zweiten enthalten sein, so muß insbesondere auch die Zahl $\frac{-b+\sqrt{D}}{2}$ eine Zahl von der Form $pz+\frac{-b-\sqrt{D}}{2}v$, d. h. $v=-1$ und $-\frac{b}{2}=pz+\frac{b}{2}$, also $b=-pz$ oder teilbar durch p sein, was nach der Kongruenz (18) nur möglich ist, wenn p ein Primteiler der Grundzahl D ist. Ist diese notwendige Bedingung aber erfüllt, so ist auch b durch p teilbar, daher ist, wenn $b=-pz$ gesetzt wird, $-\frac{b}{2}=pz+\frac{b}{2}$, also nicht nur

$$\frac{-b+\sqrt{D}}{2}=pz-\frac{-b-\sqrt{D}}{2}$$

eine im Ideale $\left[p, \frac{-b-\sqrt{D}}{2}\right]$, sondern auch

$$\frac{-b-\sqrt{D}}{2}=pz-\frac{-b+\sqrt{D}}{2}$$

eine im Ideale $\left[p, \frac{-b+\sqrt{D}}{2}\right]$ enthaltene Zahl, woraus dann folgt, daß jedes der beiden Ideale (21) durch das andere teilbar ist, und daß sie also miteinander identisch sind.

Man erkennt weiter, daß die Ideale (21), gleichviel ob identisch oder verschieden, Primideale sind. Denn, wäre das Ideal $\left[p, \frac{-b\pm\sqrt{D}}{2}\right]$ kein Primideal, so müßte es aus Primidealfaktoren zusammengesetzt, also in einem Primideale ent-

halten sein, welches, da es auch die Primzahl p enthielte, eins der Ideale (21) oder $\mathfrak{g}p$ sein müßte; das letztere ist auszuschließen, da $\frac{-b \pm \sqrt{D}}{2}$ keine Zahl dieses Ideals, nämlich nicht von der Form

$$px + py\theta = px + \frac{pyD}{2} + \frac{py\sqrt{D}}{2}$$

sein kann; also müßte das Ideal $\left[p, \frac{-b \pm \sqrt{D}}{2}\right]$ durch das andere der Ideale (21) teilbar sein, was, wie wir soeben bewiesen, nur sein kann, wenn beide identisch sind, der Primfaktor von $\left[p, \frac{-b \pm \sqrt{D}}{2}\right]$ also dies Ideal selbst ist. Die Normen der Primideale (21) sind [Kap. 1, (51)] gleich p; deshalb sollen diese Primideale als solche ersten Grades bezeichnet werden.

In diesem zweiten Falle ist aber das Ideal $\mathfrak{g}p$ kein Primideal, sondern zerfällt in das Produkt der beiden konjugierten Primideale (21). In der Tat, da p eine dem Ideale

$$\mathfrak{p} = \left[p, \frac{-b + \sqrt{D}}{2}\right] \tag{22}$$

angehörige Zahl ist, so ist mit ihr auch das Hauptideal $\mathfrak{g}p$ darin enthalten oder $\mathfrak{g}p$ teilbar durch $\mathfrak{p}$, so daß, unter $\mathfrak{j}$ ein Ideal verstanden, $\mathfrak{g}p = \mathfrak{p} \cdot \mathfrak{j}$ gesetzt werden darf. Demzufolge ergibt sich nach (17)

$$\mathfrak{N}(\mathfrak{g}p) = \mathfrak{N}(\mathfrak{j}) \cdot (\mathfrak{j}, \mathfrak{g}p);$$

mit Rücksicht auf (19) kann also $\mathfrak{N}(\mathfrak{j})$ nur einen der drei Werte $1, p, p^2$ haben. Wäre $\mathfrak{N}(\mathfrak{j}) = (\mathfrak{g}, \mathfrak{j}) = 1$, so wäre (vor. Nr.) $\mathfrak{j} = \mathfrak{g}$ und $\mathfrak{g}p = \mathfrak{p}\mathfrak{j} = \mathfrak{g}\mathfrak{p} = \mathfrak{p}$, was unmöglich ist, da, wie kurz vorher bemerkt, $\mathfrak{p}$ nicht in $\mathfrak{g}p$ enthalten, geschweige denn ihm gleich sein kann. Wäre $\mathfrak{N}(\mathfrak{j}) = p^2$, so müßte $(\mathfrak{j}, \mathfrak{g}p) = 1$, d. h. $\mathfrak{j}$ ein in $\mathfrak{g}p$ enthaltenes Ideal, mithin von der Form $\mathfrak{j}'p$ sein, wo auch $\mathfrak{j}'$ ein Ideal bedeutet, dann aber ergäbe sich $\mathfrak{g}p = \mathfrak{p}\mathfrak{j} = \mathfrak{p}\mathfrak{j}' \cdot p$, also $\mathfrak{g} = \mathfrak{p}\mathfrak{j}'$, was nicht sein kann, da $\mathfrak{g}$ keinen von sich selbst verschiedenen Idealteiler besitzt. Somit kann nur $\mathfrak{N}(\mathfrak{j}) = p$ sein, während doch $\mathfrak{j}$, da es als Teiler von $\mathfrak{g}p$ mit $\mathfrak{g}p$ auch p selbst ent-

hält, nur ein Ideal sein kann, welches entweder 1 oder p als kleinste rationale ganze Zahl enthält, somit entweder gleich $\mathfrak{g}$, oder gleich $\mathfrak{g}p$, oder eins der Ideale (21) ist; die beiden ersteren Fälle sind unvereinbar mit der Gleichung $\mathfrak{N}(j) = p$, es bleibt also nur der letzte. Demnach ergibt sich

$$\mathfrak{g}p = \mathfrak{p} \cdot \mathfrak{p}_1, \tag{23}$$

wo jeder der Faktoren eins der Ideale (21) ist. Aus demselben Grunde aber, aus welchem $\mathfrak{g}p$ durch das Ideal (22) teilbar sein mußte, ist es dies auch durch das andere, mit $\mathfrak{p}$ konjugierte Ideal (21) d. i.

$$\mathfrak{p}' = \left[p, \frac{-b-\sqrt{D}}{2}\right].$$

Wenn letzteres von $\mathfrak{p}$ verschieden, also p kein Primteiler der Grundzahl D ist, muß daher in (23) $\mathfrak{p}_1 = \mathfrak{p}'$ sein, und $\mathfrak{g}p$ ist das Produkt der beiden verschiedenen konjugierten Primideale ersten Grades $\mathfrak{p}, \mathfrak{p}'$:

$$\mathfrak{g}p = \mathfrak{p} \cdot \mathfrak{p}'.$$

Sind aber die beiden Ideale (21) identisch, d. h. ist p ein Primteiler der Grundzahl D, so erhält man aus (23)

$$\mathfrak{g}p = \mathfrak{p}^2$$

also als das Quadrat eines Primideals ersten Grades.

Diese Resultate lassen sich in folgendem eleganten, zuerst von *Dedekind* ausgesprochenen **Satze** zum Gesamtausdruck bringen:

Bedeutet p eine rationale Primzahl, welche in der Grundzahl D aufgeht, so ist $\mathfrak{g}p$ das Quadrat eines Primideals ersten Grades. Geht aber p nicht in D auf, so ist $\mathfrak{g}p$ das Produkt aus zwei voneinander verschiedenen konjugierten Primidealen ersten Grades, oder selbst ein Primideal zweiten Grades, je nachdem D quadratischer Rest oder Nichtrest ist von $4p$.

Ist insbesondere $p = 2$, so ist $\mathfrak{g}2$ das Quadrat eines Primideals ersten Grades, falls $D \equiv 0 \pmod{4}$, also $D = 4d$ ist, denn dann ist 2 ein Primteiler von D. Ist dagegen $D = d \equiv 1 \pmod{4}$, also 2 kein Primteiler von D, so zerfällt $\mathfrak{g}2$ in das Produkt zweier verschiedener, konjugierter

Primideale ersten Grades, wenn $D \equiv 1 \pmod{8}$, es ist dagegen selbst ein Primideal zweiten Grades, wenn $D \equiv 5 \pmod{8}$ ist; denn das Quadrat jeder mit D gleichartigen, also ungeraden Zahl b ist stets $\equiv 1 \pmod{8}$, also ist im ersteren und nur im ersteren Falle die Kongruenz $b^2 \equiv D \pmod{8}$ möglich.

Viertes Kapitel.

Ideale und Gitterzahlen.

1. Nachdem im Vorhergehenden für die Ideale des quadratischen Körpers die Teilbarkeitsgesetze entwickelt und als völlig übereinstimmend befunden worden sind mit denjenigen, welche die Teilbarkeit der rationalen ganzen Zahlen beherrschen, stellen wir nunmehr die gleiche Untersuchung für die einzelnen ganzen Zahlen des Körpers an. Zu diesem Zwecke wollen wir aber noch näher auf die Beziehung eingehen, die zwischen den Idealen und den quadratischen Formen schon bemerkt worden ist.

Jedes Ideal des Körpers $\mathfrak{K}$ hatte die Form eines Moduls

$$s \cdot \left[a, \frac{-b+\sqrt{D}}{2}\right], \tag{1}$$

in welchem a, b rationale, der Kongruenz $b^2 \equiv D \pmod{4a}$ genügende ganze Zahlen bedeuten, deren erstere positiv gedacht werden darf; wurde mit

$$\zeta = s\left(ax + \frac{b-\sqrt{D}}{2}y\right) \tag{2}$$

irgend eine seiner Zahlen bezeichnet, so erhielt man die Gleichung

$$N(\zeta) = s^2 a \cdot (ax^2 + bxy + cy^2), \tag{3}$$

wo $s^2 a$ die Norm des Ideals ist. Nun kann durch die primitive Form (a, b, c) stets eine Zahl m eigentlich dargestellt werden, die zu einer beliebig gegebenen Zahl M teilerfremd ist. In der Tat, sei p irgend ein in M aufgehender Primteiler, so ist notwendig wenigstens eine der Zahlen a, b, c nicht durch p teilbar; ist dies a, so wird die Form $ax^2 + bxy + cy^2$ durch p nicht teilbar, wenn man

$$x \equiv 1, \quad y \equiv 0 \pmod{p}$$

wählt; ist c nicht teilbar durch p, so geschieht das gleiche, wenn man

$$x \equiv 0, \quad y \equiv 1 \pmod{p}$$

wählt; sind aber a und c zugleich durch p teilbar, also b nicht teilbar durch p, so hat man zu gleichem Zwecke nur

$$x \equiv 1, \quad y \equiv 1 \pmod{p}$$

zu wählen; man erreicht also stets, daß die Form durch p nicht teilbar wird, indem man für jede der Zahlen x, y einen bestimmten Rest (mod. p) vorschreibt. Nun läßt sich aber sowohl x als y (nach Abschn. I, Kap. 2, Nr. 4) so angeben, daß es den verschiedenen Vorschriften, die sich so in bezug auf die einzelnen in M aufgehenden Primzahlen p ergeben, zugleich genügt; für die solcherweise bestimmten x, y wird dann der Wert der Form $ax^2 + bxy + cy^2$ durch keine jener Primzahlen teilbar, d. h. teilerfremd zu M sein. Dies wird auch so bleiben, wenn x durch $x' = x + M \cdot z$ ersetzt wird, wo z eine ganze Zahl bedeutet; da nun, wenn $f = ax'^2 + bx'y + cy^2$ gesetzt wird,

$$4af = (2ax' + by)^2 - Dy^2$$

ist, und mit wachsendem z das Quadrat $(2ax' + by)^2$ über jede Größe hinauswächst, so wird man z so groß wählen können, daß $4af$ und wegen $a > 0$ auch f selbst positiv ausfällt. Mithin können schließlich x, y in der Form $ax^2 + bxy + cy^2$ so gewählt werden, daß der Wert derselben nicht nur teilerfremd zu M, sondern auch positiv ausfällt; hätten dabei x, y einen größten gemeinsamen Teiler $\delta > 1$, so würde der durch δ^2 geteilte Wert der Form eine zu M teilerfremde positive Zahl m sein, welche durch (a, b, c) eigentlich dargestellt wird. Sei so

$$m = a\alpha^2 + b\alpha\gamma + c\gamma^2;$$

werden alsdann zwei ganze Zahlen β, δ so gewählt, daß $\alpha\delta - \beta\gamma = 1$, so geht die Form (a, b, c) durch die Transformation

$$x = \alpha x' + \beta y', \quad y = \gamma x' + \delta y'$$

in eine eigentlich äquivalente Form (m, r, n) mit positivem ersten Koeffizienten über, und dieser entspricht ein Ideal

$$s \cdot \left[m, \frac{-r + \sqrt{D}}{2}\right],$$

welches mit dem Ideale (1) äquivalent ist, oder der gleichen Idealklasse C angehört (Kap. 1, Nr. 10). Mit anderen Worten:

In jeder Idealklasse C läßt sich ein Ideal angeben — wir bezeichnen es wieder mit

$$s \cdot \left[a, \frac{-b+\sqrt{D}}{2}\right]$$

—, in welchem die Zahl a positiv und zu einer beliebig gegebenen Zahl teilerfremd ist.

2. Bezeichnen daher C_1, C_2 zwei Idealklassen, gleichviel ob diese identisch oder zwei verschiedene Klassen sind, so läßt sich ein Ideal

$$j_1 = s_1 \cdot \left[a_1, \frac{-b_1+\sqrt{D}}{2}\right]$$

der ersten Klasse und ein Ideal

$$j_2 = s_2 \cdot \left[a_2, \frac{-b_2+\sqrt{D}}{2}\right]$$

der zweiten Klasse so angeben, daß $a_1 > 0$ und ungerade und $a_2 > 0$ zu $2a_1$ teilerfremd ist. Dann gibt es aber eine Zahl B, für welche die Kongruenzen

$$(4) \qquad B \equiv b_1 \pmod{2a_1}, \qquad B \equiv b_2 \pmod{2a_2}$$

erfüllt sind, denn, da b_1, b_2 mit D, also auch untereinander gleichartig sind, kommen diese Kongruenzen auf die anderen:

$$B \equiv b_1 \equiv b_2 \pmod{2}, \quad B \equiv b_1 \pmod{a_1}, \quad B \equiv b_2 \pmod{a_2}$$

hinaus, deren Moduln zu je zweien teilerfremd sind, sie sind also (Abschn. I, Kap. 2, Nr. 4) miteinander verträglich. Für diese Zahl B ist dann auch

$$B^2 \equiv b_1^2 \equiv D \pmod{4a_1}, \qquad B^2 \equiv b_2^2 \equiv D \pmod{4a_2},$$

d. h. $B^2 - D$ sowohl durch $4a_1$ als auch durch $4a_2$ und somit auch durch $4a_1a_2$ teilbar oder

$$(5) \qquad B^2 \equiv D \pmod{4a_1a_2}.$$

Da nach (4) $B = b_1 + 2a_1\alpha_1$, $B = b_2 + 2a_2\alpha_2$ gesetzt werden kann, so ergeben sich die Gleichungen

$$a_1 x_1 + \frac{-b_1 + \sqrt{D}}{2} y_1 = a_1 z_1 + \frac{-B + \sqrt{D}}{2} y_1$$

$$a_2 x_2 + \frac{-b_2 + \sqrt{D}}{2} y_2 = a_2 z_2 + \frac{-B + \sqrt{D}}{2} y_2 ,$$

wenn $z_1 = x_1 + \alpha_1 y_1$, $z_2 = x_2 + \alpha_2 y_2$ gedacht wird, Gleichungen, aus denen ersichtlich ist, daß die Ideale j_1, j_2 auch folgendermaßen geschrieben werden können:

$$(6)\quad j_1 = s_1 \cdot \left[a_1 , \frac{-B + \sqrt{D}}{2}\right], \qquad j_2 = s_2 \cdot \left[a_2 , \frac{-B + \sqrt{D}}{2}\right].$$

Hierbei dürfen s_1, s_2 positiv gedacht werden, da $-j_1 = j_1$, $-j_2 = j_2$.

Zwei Ideale dieser Art sollen einig heißen; man darf also sagen:

Sind C_1, C_2 zwei beliebige Idealklassen, so können als ihre Repräsentanten zwei einige Ideale j_1, j_2 gewählt werden, und die ihnen entsprechenden quadratischen Formen

$$(7)\quad a_1 x^2 + Bxy + a_2 C y^2, \qquad a_2 x^2 + Bxy + a_1 C y^2 ,$$

in denen

$$(8)\quad \frac{B^2 - D}{4 a_1 a_2} = C$$

gesetzt ist, mögen gleichfalls einige Formen genannt werden.

Untersuchen wir nun das Produkt

$$j = j_1 \cdot j_2 = s_1 \cdot \left[a_1 , \frac{-B + \sqrt{D}}{2}\right] \cdot s_2 \cdot \left[a_2 , \frac{-B + \sqrt{D}}{2}\right]$$

der beiden einigen Ideale; dabei setzen wir zur Abkürzung

$$(9)\quad \Omega = \frac{-B + \sqrt{D}}{2}.$$

Da das Produkt zweier Zahlen

$$(10)\quad \zeta_1 = s_1 (a_1 x_1 - \Omega y_1), \qquad \zeta_2 = s_2 (a_2 x_2 - \Omega y_2),$$

welche den Idealen j_1, j_2 resp. angehören, gleich

$$(11)\quad \zeta_1 \zeta_2 = s_1 s_2 \cdot (a_1 a_2 x_1 x_2 - a_1 \Omega x_1 y_2 - a_2 \Omega x_2 y_1 + \Omega \Omega y_1 y_2)$$

d. i. eine Zahl des viergliedrigen Moduls

$$(12)\quad s_1 s_2 \cdot [a_1 a_2 , a_1 \Omega , a_2 \Omega , \Omega \Omega]$$

ist, so wird auch jede Summe solcher Produkte d. i. jede Zahl des Produktes $j_1 \cdot j_2$ eine Zahl des Moduls (12) sein; da aber jede der Basiszahlen

$$(13) \qquad s_1 s_2 a_1 a_2, \quad s_1 s_2 a_1 \Omega, \quad s_1 s_2 a_2 \Omega, \quad s_1 s_2 \Omega \Omega$$

des letzteren offenbar dem Produkte $j_1 \cdot j_2$ angehört, so wird auch umgekehrt jede aus Vielfachen der letzteren durch Addition entstehende Zahl, d. i. jede Zahl des Moduls (12) im Produkte $j_1 j_2$ enthalten sein und daraus ergibt sich die Gleichheit von $j_1 \cdot j_2$ mit dem Modul (12). Andererseits hat das Produkt $j_1 \cdot j_2$, weil es auch ein Ideal ist, die allgemeine Form der Ideale, etwa

$$j_1 \cdot j_2 = s \cdot \left[a, \frac{-b+\sqrt{D}}{2}\right],$$

demnach erschließen wir die Beziehung

$$(14) \; j = s \cdot \left[a, \frac{-b+\sqrt{D}}{2}\right] = s_1 s_2 \cdot [a_1 a_2, \; a_1 \Omega, \; a_2 \Omega, \; \Omega \Omega].$$

Setzt man hier $\omega = \frac{-b+\sqrt{D}}{2}$, so ergeben sich nun für die in j enthaltenen Zahlen (13) Gleichungen von der Form

$$(15) \qquad \begin{cases} s_1 s_2 a_1 a_2 = p \cdot s a + q \cdot s\omega \\ s_1 s_2 a_1 \Omega = p' \cdot s a + q' \cdot s\omega \\ s_1 s_2 a_2 \Omega = p'' \cdot s a + q'' \cdot s\omega \\ s_1 s_2 \Omega \Omega = p''' \cdot s a + q''' \cdot s\omega \end{cases}$$

mit ganzzahligen Koeffizienten $p, q, p', q', p'', q'', p''', q'''$. Da umgekehrt die Basiszahlen sa, $s\omega$ des Ideals j auch Zahlen des viergliedrigen Moduls sind, darf man

$$(16) \qquad \begin{cases} s a = s_1 s_2 a_1 a_2 \cdot t + s_1 s_2 a_1 \Omega \cdot u + s_1 s_2 a_2 \Omega \cdot v \\ \qquad\qquad + s_1 s_2 \Omega \Omega \cdot w \\ s\omega = s_1 s_2 a_1 a_2 \cdot t' + s_1 s_2 a_1 \Omega \cdot u' + s_1 s_2 a_2 \Omega \cdot v' \\ \qquad\qquad + s_1 s_2 \Omega \Omega \cdot w' \end{cases}$$

setzen, unter $t, u, v, w, t', u', v', w'$ ganze Zahlen verstanden. Vergleicht man nun in den Gleichungen (15) das

Rationale beider Seiten sowie das Irrationale, so ergibt die erste derselben

$$(17) \qquad q = 0\,, \quad s_1 s_2 a_1 a_2 = p s a$$

und die zweite und dritte

$$(18) \quad \begin{cases} s q' = s_1 s_2 a_1\,, & s q'' = s_1 s_2 a_2 \\ -Bp = 2p' a_2 - bp\,, & -Bp = 2p'' a_1 - bp\,. \end{cases}$$

Auf gleiche Weise finden sich aus der ersten der Gleichungen (16), wenn man bedenkt, daß nach (8) und (9)

$$\Omega^2 + B\Omega + C a_1 a_2 = 0\,,$$

also

$$\Omega^2 = -B\Omega - C a_1 a_2$$

ist, die folgenden:

$$s a = s_1 s_2 a_1 a_2 (t - Cw) - s_1 s_2 \cdot \frac{B}{2} (a_1 u + a_2 v - Bw)\,,$$

$$0 = s_1 s_2 (a_1 u + a_2 v - Bw)\,,$$

also

$$(19) \qquad s a = s_1 s_2 a_1 a_2 (t - Cw)\,,$$

und ebenso aus der zweiten der Gleichungen (16) diese anderen:

$$\frac{-bs}{2} = s_1 s_2 a_1 a_2 (t' - Cw') - s_1 s_2 \cdot \frac{B}{2} (a_1 u' + a_2 v' - Bw')$$

und

$$(20) \qquad s = s_1 s_2 (a_1 u' + a_2 v' - Bw')\,,$$

also

$$-b = 2pa \cdot (t' - Cw') - B\,,$$

mithin

$$(21) \qquad b \equiv B \pmod{2a}\,.$$

Da wegen der zweiten der Gleichungen (17) $s_1 s_2 a_1 a_2$ durch sa, nach (19) aber umgekehrt sa durch $s_1 s_2 a_1 a_2$ teilbar ist, ergibt sich ferner

$$(22) \qquad sa = s_1 s_2 a_1 a_2\,.$$

Aber aus (18) folgt

$$q' a_2 = q'' a_1$$

und, da a_1, a_2 relativ prim vorausgesetzt sind, müssen

$$q' = a_1 z\,, \quad q'' = a_2 z$$

sein, wo z ein ganzzahliger Faktor, und nun wegen (18)

$$s z = s_1 s_2 ,$$

also ist $s_1 s_2$ teilbar durch s; da jedoch nach (20) auch umgekehrt s teilbar ist durch $s_1 s_2$, muß

$$s = s_1 s_2 ,$$

also nach (22)

$$a = a_1 a_2$$

sein. Da endlich das Ideal j sich nicht ändert, wenn in seinem Ausdrucke b durch eine ihm (mod. $2a$) kongruente Zahl ersetzt wird, so darf man dies Ideal nunmehr schreiben, wie folgt:

$$(23) \qquad j = j_1 \cdot j_2 = s_1 s_2 \cdot \left[a_1 a_2 , \frac{-B + \sqrt{D}}{2} \right]$$

und erhält somit den **Satz:**

Das Produkt der beiden einigen Ideale (6) ist das Ideal (23).

Da nun die Normen dieser Ideale bzw.

$$\mathfrak{N}(j_1) = s_1^2 a_1 , \quad \mathfrak{N}(j_2) = s_2^2 a_2 , \quad \mathfrak{N}(j) = s_1^2 s_2^2 \cdot a_1 a_2$$

sind, geht weiter für zwei einige Ideale j_1, j_2 die Beziehung

$$(24) \qquad \mathfrak{N}(j_1 j_2) = \mathfrak{N}(j_1) \cdot \mathfrak{N}(j_2)$$

hervor.

3. Diese Beziehung gilt jedoch allgemeiner für je zwei beliebige Ideale. Sei nämlich j' ein mit j_1 äquivalentes Ideal, so daß, unter ζ eine Zahl des Körpers $\mathfrak{K}$ verstanden, $j' = \zeta_1 \cdot j_1$ gesetzt und ζ_1 als Quotient zweier ganzer Zahlen ξ, η des Körpers gedacht werden kann; wir schreiben dann

$$(25) \qquad \eta \cdot j' = \xi \cdot j_1 = \mathfrak{i} ,$$

wo auch $\mathfrak{i}$ ein Ideal bedeutet. Da nun $\xi \cdot j_1$ in dem Hauptideale $\mathfrak{g}\xi$ enthalten oder teilbar ist durch $\mathfrak{g}\xi$, so besteht nach (17) vorigen Kapitels die Beziehung

$$(26) \quad \mathfrak{N}(\mathfrak{i}) = \mathfrak{N}(\xi j_1) = \mathfrak{N}(\mathfrak{g}\xi) \cdot (\mathfrak{g}\xi, j_1 \xi) = N(\xi) \cdot (\mathfrak{g}\xi, j_1 \xi) .$$

Der letzte Faktor bedeutet die Anzahl Klassen kongruenter Zahlen, in welche die Gesamtheit $\mathfrak{g}\xi$ in bezug auf den Modul $j_1 \xi$ verteilt werden kann. Da aber offenbar die Differenz von zwei Zahlen $\gamma\xi, \gamma'\xi$ jener Gesamtheit, wo

γ, γ' zwei Zahlen in $\mathfrak{g}$ bedeuten, dann und nur dann dem Modul $j_1 \xi$ angehört, wenn die Differenz der Zahlen γ, γ' dem Modul j_1 angehört, so ist ersichtlich die Anzahl der gedachten Klassen gleich derjenigen der Klassen, in welche alle Zahlen der Gesamtheit $\mathfrak{g}$ in bezug auf den Modul j_1 verteilt werden können, d. h.

$$(\mathfrak{g}\xi, j_1 \xi) = (\mathfrak{g}, j_1) = \mathfrak{N}(j_1).$$

Die Gleichung (26) nimmt daher die Gestalt an

$$\mathfrak{N}(\mathfrak{i}) = N(\xi) \cdot \mathfrak{N}(j_1).$$

Aus (25) folgt ebenso

$$\mathfrak{N}(\mathfrak{i}) = N(\eta) \cdot \mathfrak{N}(j'),$$

daher durch Vergleichung dieser Werte und mit Rücksicht auf die Gleichheit $\zeta_1 = \frac{\xi}{\eta}$ die Beziehung

$$\mathfrak{N}(j') = N(\zeta_1) \cdot \mathfrak{N}(j_1). \tag{27}$$

Wenn nun ebenso $j'' = \zeta_2 j_2$ irgend ein mit j_2 äquivalentes Ideal bezeichnet, so daß $j'j'' = \zeta_1 \zeta_2 \cdot j_1 j_2$ mit dem Produkte $j_1 j_2$ äquivalent wird, so bestehen entsprechend die Beziehungen

$$\mathfrak{N}(j'') = N(\zeta_2) \cdot \mathfrak{N}(j_2)$$
$$\mathfrak{N}(j'j'') = N(\zeta_1 \zeta_2) \cdot \mathfrak{N}(j_1 j_2),$$

durch deren Verbindung miteinander unter Berücksichtigung von (24) sich die Formel

$$\mathfrak{N}(j'j'') = \mathfrak{N}(j') \cdot \mathfrak{N}(j'') \tag{28}$$

herausstellt, welche bewiesen werden sollte.

4. Auf Grund vorstehender Untersuchung folgern wir nun aus den Gleichungen (15), daß die Gleichung (11) die Gestalt annimmt

$$\zeta_1 \cdot \zeta_2 = s_1 s_2 (a_1 a_2 x - \Omega y),$$

wenn darin

$$\begin{cases} x = p x_1 x_2 - p' x_1 y_2 - p'' x_2 y_1 + p''' y_1 y_2 \\ y = -q x_1 x_2 + q' x_1 y_2 + q'' x_2 y_1 - q''' y_1 y_2 \end{cases} \tag{29}$$

gesetzt wird. Wegen

$$N(\zeta_1) \cdot N(\zeta_2) = N(\zeta_1 \zeta_2)$$

findet sich hieraus zwischen den zu den Idealen j_1, j_2 und $j = j_1 \cdot j_2$ zugeordneten quadratischen Formen folgende Beziehung:

$$s_1^2 a_1 (a_1 x_1^2 + B x_1 y_1 + a_2 C y_1^2) \cdot s_2^2 a_2 (a_2 x_2^2 + B x_2 y_2 + a_1 C y_2^2)$$
$$= s_1^2 s_2^2 a_1 a_2 \cdot (a_1 a_2 x^2 + B x y + C y^2)$$

oder einfacher diese andere:

$$(30) \begin{cases} (a_1 x_1^2 + B x_1 y_1 + a_2 C y_1^2)(a_2 x_2^2 + B x_2 y_2 + a_1 C y_2^2) \\ \qquad = a_1 a_2 x^2 + B x y + C y^2 . \end{cases}$$

Der Multiplikation der beiden einigen Ideale j_1, j_2 entspricht daher eine Komposition der ihnen zugeordneten einigen quadratischen Formen zu der zum Produkte $j_1 \cdot j_2$ zugeordneten quadratischen Form, d. h. eine Transformation des Produktes der beiden ersten Formen in die letztere durch eine sogenannte bilineare Substitution (29). Für die Koeffizienten dieser Substitution ergeben sich aus den Betrachtungen in Nr. 2 zunächst

$$p = 1 , \quad q = 0 , \quad q' = a_1 , \quad q'' = a_2$$

und da $b = B$ gewählt worden ist, nach (18)

$$p' = 0 , \quad p'' = 0 ;$$

aus der letzten der Gleichungen (15) findet man sodann durch Vergleichung des Rationalen sowie des Irrationalen beider Seiten leicht die Beziehungen

$$-2 s_1 s_2 a_1 a_2 C = 2 p''' s a , \quad q''' s = -B s_1 s_2 ,$$

d. h. $$p''' = -C , \quad q''' = -B .$$

Demzufolge nimmt die bilineare Substitution (29) diese Gestalt an:

$$(31) \quad \begin{cases} x = x_1 x_2 - C y_1 y_2 \\ y = a_1 x_1 y_2 + a_2 x_2 y_1 + B y_1 y_2 . \end{cases}$$

Was so für zwei einige Ideale und die ihnen entsprechenden Formen gefunden worden ist, läßt sich auf ganz dieselbe Weise, nur mit größerer Umständlichkeit für irgend zwei Ideale erweisen, und es gilt also der allgemeinere **Satz,** daß der Multiplikation zweier Ideale

$$j_1' = s_1 \left[a_1 , \frac{-b_1 + \sqrt{D}}{2} \right] , \quad j_2' = s_2 \left[a_2 , \frac{-b_2 + \sqrt{D}}{2} \right]$$

eine **Komposition** der ihnen zugeordneten Formen

$$f_1' = (a_1, b_1, c_1), \qquad f_2' = (a_2, b_2, c_2)$$

zu der ihrem Produkte $j' = j_1' \cdot j_2'$ zugeordneten quadratischen Form $f' = (a, b, c)$ entspricht; an Stelle der Gleichung (30) erhält man so die andere:

$$(a_1 x_1^2 + b_1 x_1 y_1 + c_1 y_1^2)(a_2 x_2^2 + b_2 x_2 y_2 + c_2 y_2^2) = a x^2 + b x y + c y^2,$$

worin x, y wieder mit x_1, y_1, x_2, y_2 durch eine bilineare Substitution (29), deren Koeffizienten jetzt aber andere sind, verknüpft sind, und wo für die Koeffizienten a, b, c folgende Bestimmung gilt:

Bedeutet δ den größten gemeinsamen Teiler von $a_1, a_2, \frac{b_1 + b_2}{2}$, so ist $a = \frac{a_1 a_2}{\delta^2}$ und b eine den drei Kongruenzen

$$b \cdot \frac{a_2}{\delta} \equiv b_1 \cdot \frac{a_2}{\delta}, \quad b \cdot \frac{a_1}{\delta} \equiv b_2 \cdot \frac{a_1}{\delta}, \quad b \cdot \frac{b_1 + b_2}{\delta} \equiv \frac{b_1 b_2 + D}{2\delta} \pmod{2a}$$

gleichzeitig genügende Zahl; aus den letzteren ergibt sich, wenn u, v, w drei ganze, der Gleichung

$$\frac{a_2}{\delta} \cdot u + \frac{a_1}{\delta} \cdot v + \frac{b_1 + b_2}{\delta} \cdot w = 1$$

genügende Zahlen bezeichnen, einfacher

$$b \equiv b_1 \cdot \frac{a_2}{\delta} u + b_2 \cdot \frac{a_1}{\delta} v + \frac{b_1 b_2 + D}{2\delta} \cdot w \pmod{2a} \text{ *)}.$$

Was aber an diesem Satze das wesentlichste ist und auch schon bei Beschränkung auf **einige** Ideale zutage tritt, ist der Umstand, daß die **Formenklasse** C, welcher die zusammengesetzte Form angehört, nur von den **Formenklassen** C_1, C_2 bestimmt wird, denen die zusammensetzenden Formen angehören, nicht von der willkürlichen Auswahl dieser letzteren aus ihren Klassen C_1, C_2. In der Tat, nach Kap. 1, Nr. 10 entsprechen sich die Idealklassen, denen die Ideale j_1', j_2' angehören, und die Formenklassen der ihnen

*) Siehe darüber *Dirichlets* Vorl. üb. Zahlentheorie, herausg. von *Dedekind*, 4. Aufl., S. 644 sqq., sowie *Arndt*, Journ. f. Math. v. *Crelle*, 56, S. 64.

zugeordneten quadratischen Formen f_1', f_2' in der Weise, daß, wenn j_1', j_2' durch zwei ihnen (eigentlich) äquivalente Ideale $j_1 = \zeta_1 \cdot j_1'$, $j_2 = \zeta_2 \cdot j_2'$ ersetzt werden, jene Formen bzw. mit den den letzteren Idealen zugeordneten Formen f_1, f_2 (eigentlich) äquivalent sind; da dann aber an Stelle von j' das ihm (eigentlich) äquivalente Ideal $j = j_1 j_2 = \zeta_1 \zeta_2 \cdot j'$ tritt, so wird die dem letzteren zugeordnete, nach dem allgemeinen Satze durch die Komposition von f_1, f_2 entstehende Form f in der Tat mit der dem äquivalenten Ideale j' zugeordneten, durch Komposition von f_1', f_2' entstehenden Form f' zur gleichen Klasse gehören, w. z. b. w.

Aus diesem Grunde darf die Klasse C selbst als aus den beiden Formenklassen C_1, C_2 zusammengesetzt oder als ihr Produkt

$$C = C_1 \cdot C_2$$

bezeichnet werden, und man erkennt hiernach, wie die Formenklassen in ganz der gleichen Weise und nach denselben Gesetzen komponiert werden können, wie dies in Kap. 1, Nr. 11 für die Idealklassen gezeigt worden ist, und daß dabei die Komposition der letzteren Klassen mit derjenigen der ihnen zugeordneten Formenklassen vollständig sich deckt. Insbesondere wird jede Formenklasse C zu einem bestimmten Exponenten e gehören derart, daß die Potenz C^e der Hauptklasse H gleich und unter allen Potenzen von C von dieser Beschaffenheit die niedrigste ist. Da irgend zwei Ideal- oder Formenklassen C_1, C_2, ob sie identisch oder verschieden sind, stets wieder durch Komposition eine Ideal- oder Formenklasse C ergeben, so bilden die h Klassen eine sogenannte Gruppe, und zwar, da bei der Komposition die Anordnung der Faktoren d. h. der zusammensetzenden Ideale oder Formen offenbar gleichgültig ist, eine kommutative Gruppe; zudem ist sie eine endliche Gruppe, nämlich die Anzahl ihrer Elemente endlich. Für Gruppen mit diesen Eigenschaften besteht nun ein Satz, den wir hier ohne Beweis der Gruppentheorie entnehmen müssen, und welcher in seiner Allgemeinheit zuerst von *Kronecker* begründet worden ist*). Ihm zufolge läßt sich in solchen Gruppen stets eine Anzahl von fundamentalen Elementen — hier also

*) *Kronecker* in den Monatsberichten der Berl. Akad. vom 1. Dezember 1870.

eine Anzahl von Fundamentalklassen — $K_1, K_2, \ldots, K_\lambda$ angeben, von der Beschaffenheit, daß, wenn die Exponenten, zu denen sie gehören, $e_1, e_2, \ldots, e_\lambda$ genannt werden, jedes Element der Gruppe — jede Klasse C — als Produkt von Potenzen jener fundamentalen Elemente — Fundamentalklassen — eindeutig ausgedrückt werden kann, und daß so der Ausdruck

$$C = K_1^{h_1} \cdot K_2^{h_2} \ldots K_\lambda^{h_\lambda}, \tag{32}$$

wenn die Exponenten darin resp. die Werte

$$\begin{aligned} h_1 &= 1, 2, 3, \ldots, e_1, \\ h_2 &= 1, 2, 3, \ldots, e_2, \\ &\cdot \; \cdot \; \cdot \; \cdot \; \cdot \; \cdot \; \cdot \; \cdot \\ h_\lambda &= 1, 2, 3, \ldots, e_\lambda \end{aligned}$$

durchlaufen, sämtliche h Elemente der Gruppe (sämtliche Klassen) erzeugt, und demnach $h = e_1 e_2 \ldots e_\lambda$ ist.

5. Wir wenden uns nun dazu, dieser Zusammensetzung der Formenklassen ihre geometrische Deutung zu geben, wie sie aus der früher gelehrten anschaulichen Darstellung der quadratischen Formen selbst sich ergibt. Jeder quadratischen Form entsprach ein Parallel- oder Punktgitter, dessen Gitterpunkte, die Träger der zur Form gehörigen Gitterzahlen, durch die letzteren bestimmt sind, und welches als geometrisches Bild nicht nur der Form selbst, sondern allgemeiner der Klasse, der sie angehört, anzusehen war. Wenn man daher aus den h Formenklassen je eine Form als ihren Repräsentanten auswählt, wobei als Repräsentant der Hauptklasse die Hauptform gewählt werde, so erhält man h Gitter, die wir auf dieselbe Ebene und zunächst alle mit den gleichen Achsen OX, OY übereinandergelegt denken wollen. Dasjenige Gitter, welches die Hauptklasse repräsentiert, heiße Hauptgitter, die übrigen Nebengitter. Seien so

$$a_1 x_1^2 + b_1 x_1 y_1 + c_1 y_1^2, \quad a_2 x_2^2 + b_2 x_2 y_2 + c_2 y_2^2 \tag{33}$$

zwei der repräsentierenden Formen mit positiven ersten Koeffizienten und bezeichnen G_1, G_2 ihre Gitter, ferner

$$j_1 = s_1 \cdot \left[a_1, \frac{-b_1 + \sqrt{D}}{2}\right], \quad j_2 = s_2 \cdot \left[a_2, \frac{-b_2 + \sqrt{D}}{2}\right] \tag{34}$$

[illegible]

[illegible] Wenn [illegible] so erhält [illegible] die Zahlen von [illegible] das aus [illegible] das aus [illegible] zusammen- [illegible] der beiden [illegible] G_3 [illegible] der Multiplication zweier

Ideale j_1, j_2 oder der Komposition der ihnen zugeordneten Formen (33) eine Komposition der die letzteren repräsentierenden Gitter G_1, G_2 zu einem neuen Gitter G, welches dem aus den Idealen j_1, j_2 durch Multiplikation entstehenden Ideale j oder der ihm zugeordneten durch Komposition aus den Formen (33) entstehenden Form oder deren Klasse zum geometrischen Abbilde dient, doch ist der Multiplikator, mit dem seine Gitterzahlen multipliziert auftreten, nicht willkürlich, sondern durch diejenigen der Gitter G_1, G_2 bestimmt, nämlich gleich deren Produkte $\varrho_1 \cdot \varrho_2$. Der Schlußsatz vor. Nr. zeigt, daß, wenn wir für die Gitter Γ_i der die Fundamentalklassen K_i repräsentierenden Formen die Multiplikatoren nach Willkür gewählt haben, sie dadurch auch für die Gitter jedes der anderen Klassenrepräsentanten bestimmt sind. Es kommt aber darauf an, sie so zu wählen, daß die Gesetze der Komposition der Formen auch für diejenige ihrer Gitter in Geltung verbleiben.

6. Hierbei müssen wir die Fälle einer negativen und positiven Diskriminante gesondert behandeln. In beiden Fällen aber wollen wir das Hauptgitter unverändert lassen, nämlich den Multiplikator $\varrho = 1$, d. h. als Gitterzahlen, welche die Koordinaten dieses Punktgitters bestimmen, die ganzen Zahlen des Körpers $\mathfrak{K}$ wählen.

Sei dann im ersteren Falle Γ_1 das Gitter, welches der Fundamentalklasse K_1 entspricht, deren Repräsentanten wir mit

$$a_1 x_1^2 + b_1 x_1 y_1 + c_1 y_1^2$$

bezeichnen; die zugehörigen Gitterzahlen haben die Form

$$\eta_1 = \varrho_1 \xi_1 = \varrho_1 \left(\sqrt{a_1} \cdot x_1 + \frac{b_1 - \sqrt{D}}{2\sqrt{a_1}} \cdot y_1 \right),$$

$$\eta_1' = \varrho_1^{-1} \xi_1' = \varrho_1^{-1} \left(\sqrt{a_1} \cdot x_1 + \frac{b_1 + \sqrt{D}}{2\sqrt{a_1}} \cdot y_1 \right).$$

Wird nun die Klasse K_1 und damit auch ihr Gitter Γ_1 e_1 mal mit sich selbst zusammengesetzt, so geht die besondere Gitterzahl $\varrho_1 \cdot \sqrt{a_1}$, die den Werten $x_1 = 1$, $y_1 = 0$ entspricht in $\varrho_1^{e_1} \cdot \sqrt{a_1^{e_1}}$ über; da aber $K_1^{e_1} = H$ d. i. gleich der Hau[illegible] klasse ist, deren Gitterzahlen die ganzen Zahlen des qu[illegible] dratischen Körpers sind, so muß vorstehendes Produkt ein

solchen Zahl gleich und der ihm entsprechende Punkt des zusammengesetzten Gitters ein Punkt des Hauptgitters mit den Gitterzahlen $\varrho_1^{e_1}\sqrt{a_1^{e_1}}$, $\varrho_1^{-e_1}\sqrt{a_1^{e_1}}$ sein, sich also auf einem um den Anfangspunkt O mit dem Radius $\sqrt{a_1^{e_1}}$ beschriebenen Kreise befinden und in seiner Lage auf dem letzteren durch sein sogenanntes Azimut, d. i. durch den Winkel ψ_1 bestimmt sein, den der von O nach ihm gehende Radius mit der Achse OX bildet; seine Koordinaten sind demnach $\sqrt{a_1^{e_1}}\cdot\cos\psi_1$, $\sqrt{a_1^{e_1}}\cdot\sin\psi_1$ und demnach seine Gitterzahlen gleich

$$\sqrt{a_1^{e_1}}\cdot(\cos\psi_1 \pm i\sin\psi_1) = \sqrt{a_1^{e_1}}\cdot e^{\pm i\psi_1}.$$

Durch Vergleichung mit $\varrho_1^{e_1}\cdot\sqrt{a_1^{e_1}}$ findet man also $\varrho_1^{e_1} = e^{i\psi_1}$ mithin etwa

$$\varrho_1 = e^{i\cdot\frac{\psi_1}{e_1}}.$$

Damit also die Zusammensetzung der Gitter mit derjenigen der Klassen in Übereinstimmung sei, soll der Multiplikator für das Gitter Γ_1 in der angegebenen Weise gewählt und

$$\eta_1 = e^{i\cdot\frac{\psi_1}{e_1}}\left(\sqrt{a_1}\cdot x_1 + \frac{b_1-\sqrt{D}}{2\sqrt{a_1}}\cdot y_1\right)$$

gesetzt werden. Dies kann in einfachster Weise geometrisch gedeutet werden. Bestimmt man nämlich das zur Klasse K_1 oder zu ihrem Repräsentanten (a_1, b_1, c_1) gehörige Gitter wie ursprünglich durch die Gitterzahlen

$$\xi_1 = \sqrt{a_1}\cdot x_1 + \frac{b_1-\sqrt{D}}{2\sqrt{a_1}}\cdot y_1, \quad \xi_1' = \sqrt{a_1}\cdot x_1 + \frac{b_1+\sqrt{D}}{2\sqrt{a_1}}\cdot y_1,$$

so finden sich die Koordinaten X, Y der Gitterpunkte aus der Gleichung

$$X + Yi = r(\cos\varphi + i\sin\varphi) = \xi_1;$$

wenn aber statt ξ_1, ξ_1' die Werte $\varrho_1\xi_1$, $\varrho_1^{-1}\xi_1'$ als Gitterzahlen eingeführt werden, so bestimmen sich die Koordinaten X', Y' der Gitterpunkte durch die Gleichung

$$X' + Y'\cdot i = \varrho_1 r(\cos\varphi + i\sin\varphi)$$

$$= re^{i\frac{\psi_1}{e_1}}(\cos\varphi + i\sin\varphi) = r\left(\cos\left(\varphi + \frac{\psi_1}{e_1}\right) + i\sin\left(\varphi_1 + \frac{\psi_1}{e_1}\right)\right).$$

Der Punkt X', Y' liegt daher auf demselben Kreise wie der Punkt X, Y, doch um den Bogen $\frac{\psi_1}{e_1}$ verschoben. Die Einführung des angegebenen Multiplikators ϱ_1 in die Gitterzahlen kommt also geometrisch darauf hinaus, daß das ursprüngliche Gitter um den Winkel $\frac{\psi_1}{e_1}$ um O gedreht oder im Azimute $\frac{\psi_1}{e_1}$ gegen das Hauptgitter orientiert wird.

Was für das eine Fundamentalgitter Γ_1 gilt, gilt in entsprechender Weise für die übrigen auch. Man erhält also für die Multiplikatoren dieser Gitter $\Gamma_1, \Gamma_2, \ldots, \Gamma_\lambda$ Zahlen von der Form

$$\varrho_1 = e^{i\cdot\frac{\psi_1}{e_1}}, \quad \varrho_2 = e^{i\cdot\frac{\psi_2}{e_2}}, \ \ldots, \quad \varrho_\lambda = e^{i\cdot\frac{\psi_\lambda}{e_\lambda}},$$

d. h. für alle diese Gitter eine ganz bestimmte Orientierung gegen das Hauptgitter. Aus dieser Orientierung der Fundamentalgitter folgt dann aus (32) ohne weiteres auch für das jeder anderen Klasse C entsprechende Gitter Γ der einzuführende Multiplikator

$$\varrho = e^{i\left(\frac{h_1\psi_1}{e_1} + \frac{h_2\psi_2}{e_2} + \ldots + \frac{h_\lambda\psi_\lambda}{e_\lambda}\right)}$$

oder die für dasselbe erforderliche Orientierung gegen das Hauptgitter im Azimute

$$\psi = \frac{h_1\psi_1}{e_1} + \frac{h_2\psi_2}{e_2} + \ldots + \frac{h_\lambda\psi_\lambda}{e_\lambda}.$$

So entsteht aus der ursprünglichen Figur, in welcher die den sämtlichen h Klassen entsprechenden Gitter mit gleichen Achsen übereinandergelegt wurden, eine andere — wir nennen sie die Normalfigur — bei welcher diese Gitter in bestimmter Orientierung gegen das Hauptgitter aufeinander gelagert sind. Diese orientierten Gitter erfüllen dann aber die gestellte Bedingung, daß durch die Zusammensetzung irgend zweier derselben wieder eins von ihnen in der ihm eigentümlichen Orientierung entsteht, und daher die Zusammensetzung der Gitter derjenigen der Klassen, welche sie repräsentieren, völlig konform wird. In der Tat, sei

$$C' = K_1^{h_1'} \cdot K_2^{h_2'} \ldots K_\lambda^{h_\lambda'}$$

eine zweite Klasse und Γ' das ihr entsprechende orientierte Gitter, so daß dessen Azimut und Multiplikator

$$\psi' = \frac{h_1' \psi_1}{e_1} + \frac{h_2' \psi_2}{e_2} + \ldots + \frac{h_\lambda' \psi_\lambda}{e_\lambda},$$

$$\varrho' = e^{\psi' i}$$

sind. Hieraus folgt für den Multiplikator des aus Γ, Γ' zusammengesetzten Gitters die Gleichung

$$\varrho'' = \varrho \cdot \varrho' = e^{\psi i} \cdot e^{\psi' i} = e^{(\psi + \psi') i}$$

und somit für sein Azimut

$$\psi'' = \psi + \psi'.$$

Dies ist aber in der Tat das Azimut für das der zusammengesetzten Klasse

$$C \cdot C' = K_1^{h_1 + h_1'} \cdot K_2^{h_2 + h_2'} \ldots K_\lambda^{h_\lambda + h'_\lambda}$$

entsprechende Gitter, nämlich

$$\psi'' = \frac{(h_1 + h_1') \psi_1}{e_1} + \frac{(h_2 + h_2') \psi_2}{e_2} + \ldots + \frac{(h_\lambda + h_\lambda') \psi_\lambda}{e_\lambda}.$$

7. Im zweiten Fall einer positiven Diskriminante gelten völlig entsprechende Betrachtungen, nur daß ihm die gleiche einfache geometrische Deutung fehlt, welche der vorige Fall zuließ. Auch jetzt geht, wenn das Gitter Γ_1 $e_1$mal mit sich selbst zusammengesetzt wird, die besondere Gitterzahl $\varrho_1 \cdot \sqrt{a_1}$ einerseits über in $\varrho_1^{e_1} \cdot \sqrt{a_1^{e_1}}$, andererseits in eine der Hauptzahlen, also ist der dem vorstehenden Produkte entsprechende Punkt des zusammengesetzten Gitters ein Punkt des Hauptgitters, welcher die Gitterzahlen $\varrho_1^{e_1} \cdot \sqrt{a_1^{e_1}}$, $\varrho_1^{-e_1} \cdot \sqrt{a_1^{e_1}}$, also den hyperbolischen Abstand $\sqrt{a_1^{e_1}}$ von O hat. Sind X, Y seine Koordinaten und δ, δ' seine Abstände von den Winkelhalbierenden $U \mp V = 0$, so bestehen die Gleichungen

$$\delta = \frac{X - Y}{\sqrt{2}}, \quad \delta' = \frac{X + Y}{\sqrt{2}}$$

und die Gitterzahlen jenes Punktes sind $\xi = \delta\sqrt{2}$, $\xi' = \delta'\sqrt{2}$. Durch Vergleichung mit den obigen Werten derselben

ergibt sich folglich für den Multiplikator ϱ_1 die Bestimmung

$$\varrho_1 = \left(\frac{\delta\sqrt{2}}{\sqrt{a_1^{e_1}}}\right)^{\frac{1}{e_1}},$$

die zu einer vollständigen wird, wenn der positive Wert dieser e_1 ten Wurzel gewählt wird. Eine analoge Bestimmung erhält man für den Multiplikator eines jeden der anderen Fundamentalgitter und nach (32) daraus folgend auch die Bestimmung desselben für das Gitter jeder der übrigen Klassen. Hat man aber in solcher Weise die Multiplikatoren festgelegt, so ergibt sich wieder aus dem allgemeinen in (32) ausgesprochenen Satze von der Zusammensetzung der Klassen der gleiche Umstand wie im vorigen Falle, daß nämlich die Zusammensetzung der mittels der angegebenen Multiplikatoren „orientierten", d. i. aus den ursprünglichen Gittern entstandenen Gitter derjenigen der Klassen, welche sie repräsentieren, vollkommen konform ist.

8. Zum Schluß dieser Erörterungen erinnern wir daran (Kap. 1, Nr. 13), daß mit jeder Klasse C eine bestimmte andere Klasse C' (ihre Reziproke) verbunden ist durch den Umstand, daß die zusammengesetzte Klasse $C \cdot C'$ der Hauptklasse H gleich ist, nämlich, wenn C zum Exponenten e gehört, so daß $C^e = H$ ist, die Klasse $C' = C^{e-1}$. Ist (a, b, c) der Repräsentant der Klasse C, also

$$\eta = \varrho\left(\sqrt{a}\cdot x + \frac{b-\sqrt{D}}{2\sqrt{a}}\cdot y\right)$$

die Gitterzahl für das entsprechende orientierte Gitter Γ, so wird die Klasse C' durch die jener Form entgegengesetzte Form $(a, -b, c)$ repräsentiert. In der Tat besteht die Beziehung

$$\left(\sqrt{a}\cdot x + \frac{b-\sqrt{D}}{2\sqrt{a}}\cdot y\right)\left(\sqrt{a}\cdot x' - \frac{b+\sqrt{D}}{2\sqrt{a}}\cdot y'\right)$$
$$= \left(a x x' - c y y' + b\cdot\frac{y x' - x y'}{2}\right) - \frac{y x' + x y'}{2}\cdot\sqrt{D},$$

deren rechte Seite, falls $D = 4d$, also b gerade ist, in

$$X + Y\sqrt{d}$$

übergeht, wenn

$$X = a x x' - c y y' + \frac{b}{2}(y x' - x y'), \quad Y = -(y x' + x y')$$

gesetzt wird, während sie, falls $D = d \equiv 1 \pmod{4}$, also b ungerade ist, sich in

$$X + Y \cdot \frac{1 + \sqrt{d}}{2}$$

verwandelt, wenn

$$X = a x x' - c y y' + \frac{b+1}{2} x y' - \frac{b-1}{2} x' y,$$

$$Y = -(y x' + x y')$$

gesetzt wird; in beiden Fällen bezeichnen X, Y zugleich mit x, y, x', y' ganze Zahlen. Hieraus folgt aber die Formel

$$(a x^2 + b x y + c y^2)(a x'^2 - b x' y' + c y'^2) = X^2 - d Y^2$$

bzw.

$$(a x^2 + b x y + c y^2)(a x'^2 - b x' y' + c y'^2) = X^2 + X Y + \frac{1-d}{4} Y^2,$$

welche lehrt, daß durch Zusammensetzung der beiden entgegengesetzten Formen die Hauptform entsteht und somit die Form $(a, -b, c)$ zu der zur Klasse C der Form (a, b, c) reziproken Klasse gehören muß; übrigens kann es geschehen, daß diese Klasse C' mit der Klasse C identisch ist; man nennt in diesem Falle die Klasse C eine Ambige oder (nach *Gauß*) eine classis anceps. Da nun die Gitterzahl jener Form

$$\varrho' \left(\sqrt{a} \cdot x' - \frac{b + \sqrt{D}}{2\sqrt{a}} \cdot y' \right)$$

ist, so muß in dem orientierten Gitter Γ' der Klasse C' der Multiplikator $\varrho' = \varrho^{-1}$ sein, damit bei der Zusammensetzung von C und C' der der Hauptklasse entsprechende Multiplikator $\varrho' \cdot \varrho = 1$ hervorgeht, und demnach wird

$$\eta' = \varrho^{-1} \cdot \left(\sqrt{a} \cdot x' - \frac{b + \sqrt{D}}{2\sqrt{a}} \cdot y' \right)$$

die Gitterzahl des orientierten Gitters Γ' sein. Man sieht, daß die Gitterzahlen von Γ', abgesehen vom Multiplikator und von der verschiedenen Bezeichnung der Unbestimmten, die konjugierten, nämlich durch Vertauschung des Vorzeichens von $\sqrt{D}$ hervorgehenden Werte zu den Gitterzahlen von Γ sind; aus diesem Grunde mögen die Gitter Γ, Γ' selbst konjugierte Gitter genannt werden.

9. Nachdem wir im Vorhergehenden das geometrische Gebilde, welches wir die Normalfigur genannt haben, im Anschluß an *F. Klein*, der es zuerst angegeben hat und dessen Ausführungen diesen Nummern zugrunde liegen,*) konstruiert haben, betrachten wir nunmehr die Gesamtheit $\mathfrak{G}$ aller Gitterzahlen, deren Träger die Punkte jenes Gebildes sind, und wollen die Gesetze feststellen, durch welche die Teilbarkeit in dieser Gesamtheit beherrscht wird. Da zu der letzteren insbesondere auch die Gesamtheit $\mathfrak{g}$ der ganzen algebraischen Zahlen des quadratischen Körpers $\mathfrak{K}$ gehört, erlangen wir so zugleich auch die Teilbarkeitsgesetze für die letzteren und damit die Lösung der Aufgabe, die wir in Nr. 1 dieses Kapitels gestellt haben.

Das erste, was wir zu bemerken haben, ist die aus der Konstruktion der Normalfigur unmittelbar folgende Tatsache, daß das Produkt zweier Zahlen der Gesamtheit $\mathfrak{G}$ stets wieder eine ihrer Zahlen ist. Ferner ist leicht einzusehen, daß alle Zahlen in $\mathfrak{G}$ ganze algebraische Zahlen sind. In der Tat, ist η eine Zahl des Gitters Γ, welches das Bild einer zum Exponenten e gehörigen Klasse C ist, so ist die durch $e$malige Zusammensetzung dieses Gitters gebildete Zahl η^e eine dem Hauptgitter angehörige Zahl, d. h. eine ganze Zahl γ des quadratischen Körpers, die folglich einer ganzzahligen quadratischen Gleichung von der Form

$$z^2 + Az + B = 0$$

Genüge leistet, derart daß identisch

$$\gamma^2 + A\gamma + B = 0,$$

also

$$\eta^{2e} + A\eta^e + B = 0,$$

mithin η Wurzel der ganzzahligen Gleichung

$$z^{2e} + Az^e + B = 0,$$

*) S. seine ausgew. Kap. der Zahlentheorie II, 2. Hauptteil.

d. i. eine ganze algebraische Zahl ist. Da jedoch die Nebengitterzahlen keine Zahlen des quadratischen Körpers sind, wollen wir sie im Gegensatze zu den Hauptgitterzahlen, d. h. zu den ganzen Zahlen des Körpers als ideale Zahlen des letzteren bezeichnen.

Wir nennen nun eine Zahl η der Gesamtheit $\mathfrak{G}$ teilbar durch eine Zahl η_1 derselben, wenn eine ganze algebraische Zahl η_2 angebbar ist, so daß $\eta = \eta_1 \cdot \eta_2$ wird. Diese Zahl η_2 muß dann aber auch eine Zahl in $\mathfrak{G}$ sein. Sei nämlich

$$\eta_1 = \varrho_1\left(\sqrt{a_1}\cdot x_1 + \frac{b_1 - \sqrt{D}}{2\sqrt{a_1}}\cdot y_1\right),$$

also

$$\eta = \varrho_1\left(\sqrt{a_1}\cdot x_1 + \frac{b_1 - \sqrt{D}}{2\sqrt{a_1}}\cdot y_1\right)\cdot \eta_2,$$

so ergibt sich daraus durch Multiplikation mit der zu η_1 konjugierten Zahl

$$\eta_1' = \varrho_1^{-1}\left(\sqrt{a_1}\cdot x_1 + \frac{b_1 + \sqrt{D}}{2\sqrt{a_1}}\cdot y_1\right),$$

da $\eta_1 \cdot \eta_1' = a_1 x_1^2 + b_1 x_1 y_1 + c_1 y_1^2$, also eine rationale ganze Zahl ist, welche r heiße, die Gleichung

$$r\eta_2 = \eta \cdot \eta_1',$$

in welcher das Produkt zur Rechten eine gewisse Zahl in $\mathfrak{G}$, also von der Form

$$\varrho\left(\sqrt{a}\cdot x + \frac{b - \sqrt{D}}{2\sqrt{a}}\cdot y\right)$$

ist. Demnach wäre

$$\eta_2 = \varrho\left(\sqrt{a}\cdot\frac{x}{r} + \frac{b - \sqrt{D}}{2\sqrt{a}}\cdot\frac{y}{r}\right), \tag{39}$$

und die Behauptung kommt darauf hinaus, daß hier die Zahlen $\frac{x}{r}$, $\frac{y}{r}$ ganze Zahlen sein müssen. Um dies zu beweisen, zeigen wir allgemein, daß ein Ausdruck

$$\varrho\left(\sqrt{a}\cdot x + \frac{b - \sqrt{D}}{2\sqrt{a}}\cdot y\right) \tag{40}$$

nur dann eine ganze algebraische Zahl sein kann, wenn die Unbestimmten x, y ganzzahlige Werte haben. Multipliziert man nämlich den Ausdruck (40) mit den sämtlichen Werten des zum konjugierten Gitter gehörigen Ausdrucks

$$\varrho^{-1}\left(\sqrt{a}\cdot x' - \frac{b+\sqrt{D}}{2\sqrt{a}}\cdot y'\right), \tag{41}$$

welche ganzzahligen Werten von x', y' entsprechen, so ist das Produkt von einer der beiden Formen

$$X + Y\sqrt{d} \quad \text{oder} \quad X + Y\cdot\frac{1+\sqrt{d}}{2}, \tag{42}$$

wo

$$Y = -(xy' + x'y)$$

ist (vor. Nr.). Dies Produkt muß aber, wenn (40) eine ganze algebraische Zahl ist, ebenfalls eine solche sein, welche ganzzahligen Werte x', y' auch haben, da für solche der Ausdruck (41) stets eine ganze algebraische Zahl, nämlich eine Zahl in $\mathfrak{G}$ ist. Demnach müssen dann auch X, Y stets ganze rationale Zahlen sein; man findet aber für $x' = -1$, $y' = 0$ den Wert $Y = y$, für $x' = 0$, $y' = -1$ den Wert $Y = x$; daher müssen auch, wie behauptet, x, y ganze Zahlen sein. — Aus dieser Tatsache ist aber zu schließen, daß auch in (39) die Quotienten $\frac{x}{r}$, $\frac{y}{r}$ ganze Zahlen sind, und somit η_2 eine der Zahlen in $\mathfrak{G}$ ist, w. z. b. w.

10. Nach der innigen Beziehung, in welcher die Gitter der quadratischen Formen und folglich auch die idealen Zahlen des Körpers zu seinen Idealen stehen, läßt sich im voraus erwarten, daß die Teilbarkeitsgesetze, die wir für diese, aus den wirklichen Zahlen des Körpers d. i. den Zahlen in $\mathfrak{g}$ gebildeten Moduln gefunden haben, sich auch auf die Teilbarkeit der idealen Zahlen übertragen werden. Dies wird sich durch unsere weiteren Betrachtungen vollkommen bestätigen.

Jedem Ideale ist eine quadratische Form, also auch deren Klasse und das sie repräsentierende Gitter der Normalfigur und dessen Gitterzahlen zugeordnet. Aber es besteht auch zwischen jeder einzelnen dieser Zahlen und einem ganz bestimmten Ideale des Körpers eine Zusammengehörig-

keit, der zufolge man das Ideal aus der idealen Zahl erzeugt nennen darf.

Ist nämlich

$$\eta = \varrho\left(\sqrt{a}\cdot x + \frac{b-\sqrt{D}}{2\sqrt{a}}\cdot y\right)$$

eine Zahl des Gitters Γ, so ist, wie in vor. Nr. gezeigt, das Produkt aus η in eine Zahl η_1' des konjugierten Gitters Γ', d. i. in eine Zahl (41) eine Zahl von der Form (42), also eine Zahl in $\mathfrak{g}$, und die Gesamtheit all dieser Produkte, welche den sämtlichen Zahlen des Gitters Γ' entsprechen, ist ein Ideal j des quadratischen Körpers. In der Tat, wird eine Zahl eines beliebigen Gitters mit einer Zahl des Hauptgitters d. i. der Gesamtheit $\mathfrak{g}$ multipliziert, so entsteht ersichtlich wieder eine Zahl jenes Gitters, da jede Klasse durch Zusammensetzung mit der Hauptklasse unverändert bleibt. Ist also $\eta\cdot\eta_1'$ eins der gedachten Produkte und γ irgend eine Zahl in $\mathfrak{g}$, so ist auch $\eta_1'\gamma$ eine Zahl des obengedachten konjugierten Gitters und deshalb $\eta\cdot\eta_1'\gamma = \eta\,\eta_1'\cdot\gamma$ eins jener Produkte, deren Gesamtheit wir j genannt haben, und welche also — wie offenbar — einen Modul ganzer Zahlen des Körpers, und zwar mit der charakteristischen Eigenschaft der Ideale darstellt. Dies Ideal j heiße d a s a u s d e r Z a h l η e r z e u g t e I d e a l und werde als solches genauer durch

$$j(\eta) = \eta\cdot\Gamma'$$

bezeichnet.

11. Sein eigentliches Verhältnis zur erzeugenden Gitterzahl aber wird durch den **Satz** ausgesprochen, daß d i e s I d e a l $j(\eta)$ d i e G e s a m t h e i t a l l e r d u r c h d i e G i t t e r z a h l η t e i l b a r e n Z a h l e n i n $\mathfrak{g}$ s e i. Dies leuchtet für den besonderen Fall, daß η eine Zahl des Hauptgitters, also selbst eine Zahl γ in $\mathfrak{g}$ ist, unmittelbar ein, denn dann ist das konjugierte Gitter ebenfalls das Hauptgitter, da die Hauptklasse nach der Gleichung $H\cdot H = H$ sich selbst konjugiert ist, und demnach ist das aus γ erzeugte Ideal $j(\gamma)$ die Gesamtheit aller Produkte aus γ in die Zahlen des Hauptgitters oder in die ganzen Zahlen des Körpers und ist daher mit dem Hauptideale $\mathfrak{g}\gamma$ identisch, welches aus den durch γ teilbaren Zahlen in $\mathfrak{g}$ besteht. Um aber den Satz allgemein zu erweisen, bemerke man einerseits, daß nach

der Bildung des Ideals $j(\eta)$ seine Zahlen jedenfalls sämtlich durch η teilbar und zu $\mathfrak{g}$ gehörig sind; aber andererseits muß auch jede durch η teilbare Zahl in $\mathfrak{g}$ dem Ideal $j(\eta)$ angehören. Denn, ist $\gamma = \eta \cdot \eta_1$ eine durch η teilbare Zahl in $\mathfrak{g}$, mithin η_1 eine Gitterzahl (Nr. 9), so folgt durch Multiplikation mit der zu η konjugierten Zahl η', wenn wieder $\eta \cdot \eta' = r$ gesetzt wird,

$$r \cdot \eta_1 = \eta' \cdot \gamma,$$

wo rechts eine Zahl des zum Gitter Γ von η konjugierten Gitters Γ' steht, welche

$$\varrho^{-1}\left(\sqrt{a} \cdot x_1 - \frac{b + \sqrt{D}}{2\sqrt{a}} \cdot y_1\right)$$

heiße, folglich wird

$$\eta_1 = \varrho^{-1}\left(\sqrt{a} \cdot \frac{x_1}{r} - \frac{b + \sqrt{D}}{2\sqrt{a}} \cdot \frac{y_1}{r}\right),$$

wo nun, da η_1 ganze Zahl sein soll, die Quotienten $\frac{x_1}{r}$, $\frac{y_1}{r}$ ganze Zahlen sein müssen, sich also η_1 als eine Zahl des Gitters Γ' und daher γ sich als eine Zahl des aus η erzeugten Ideals ergibt.

Hieraus geht weiter hervor, daß eine gegebene Gitterzahl η auch nur ein Ideal erzeugen kann, denn die Gesamtheit aller ganzen Zahlen des Körpers, welche durch η teilbar sind, ist eben nur eine eindeutig bestimmte. Dies kommt auf die beachtenswerte Tatsache hinaus, daß die verschiedenen Gitter außer dem Punkt 0 keinen gemeinsamen Punkt haben können, denn sonst gehörte die von ihm getragene Gitterzahl η zwei verschiedenen Gittern Γ, Γ_1 an und gäbe, mit den Zahlen der zu diesen konjugierten Gittern Γ', Γ_1' zusammengesetzt, zwei offenbar verschiedene Ideale $\eta \cdot \Gamma'$ und $\eta \cdot \Gamma_1'$ gegen das Bemerkte.

12. Wenn nun jede Gitterzahl auf dem angegebenen Wege ein bestimmtes Ideal erzeugt, so läßt sich noch weiter zeigen, daß so auch sämtliche Ideale des Körpers hervorgebracht werden. In der Tat hat jedes Ideal die Form

$$s \cdot \left[a, \frac{-b + \sqrt{D}}{2}\right], \tag{43}$$

worin $b^2 \equiv D \pmod{4a}$, seine sämtlichen Zahlen sind also

$$s \cdot \left(ax + \frac{b-\sqrt{D}}{2}y\right) = \varrho s \sqrt{a} \cdot \varrho^{-1}\left(\sqrt{a} \cdot x + \frac{b-\sqrt{D}}{2\sqrt{a}} \cdot y\right).$$

Hier ist $\varrho s \sqrt{a}$ eine Zahl von der Form

$$\varrho\left(\sqrt{a} \cdot x - \frac{b+\sqrt{D}}{2\sqrt{a}} \cdot y\right),$$

d. i. eine Zahl eines Gitters Γ, zu welchem das Gitter Γ' der Zahlen von der Form

$$\varrho^{-1}\left(\sqrt{a} \cdot x + \frac{b-\sqrt{D}}{2\sqrt{a}} \cdot y\right)$$

konjugiert ist. Die Zahlen des Ideals (43) entstehen also aus der Zahl $\eta = \varrho s \sqrt{a}$ des Gitters Γ durch Zusammensetzung mit allen Zahlen des konjugierten Gitters Γ', und daher wird das Ideal aus der Gitterzahl η erzeugt oder gleich $j(\eta)$.

Indessen braucht η nicht die einzige Zahl zu sein, von welcher es erzeugt wird. Wir wollen eine Gitterzahl ε eine Einheit in $\mathfrak{G}$ nennen, wenn sie das besondere Ideal $\mathfrak{g}$ erzeugt. Da dies letztere dann die Gesamtheit aller ganzen Zahlen des Körpers ist, welche durch ε teilbar sind, und da die Eins in $\mathfrak{g}$ enthalten ist, so ist offenbar ε ein Teiler von 1; umgekehrt, wenn die Gitterzahl ε solch Teiler ist, so ist auch jede ganze Zahl $\gamma = 1 \cdot \gamma$ des Körpers teilbar durch ε und somit das von ε erzeugte Ideal gleich $\mathfrak{g}$. Man darf demnach die Einheiten der Gesamtheit $\mathfrak{G}$ auch als diejenigen ihrer Zahlen definieren, welche Teiler der Eins sind.

Dies vorausgeschickt läßt sich beweisen, daß alle assoziierten, d. h. nur um solche Einheitsfaktoren voneinander verschiedenen Gitterzahlen und nur sie ein- und dasselbe Ideal erzeugen. Es besteht nämlich folgender **Satz:** Ist eine Gitterzahl η das Produkt zweier Gitterzahlen η_1, η_2, so ist das vom Produkte $\eta = \eta_1 \cdot \eta_2$ erzeugte Ideal gleich dem Produkte der von den Faktoren erzeugten Ideale, in Zeichen:

$$(44) \qquad j(\eta) = j(\eta_1 \eta_2) = j(\eta_1) \cdot j(\eta_2).$$

Denn, bezeichnen Γ, Γ_1, Γ_2 die orientierten Gitter, denen die Zahlen η, η_1, η_2 resp. angehören, so ist Γ das zusammengesetzte Gitter $\Gamma_1 \cdot \Gamma_2$, denn es hat mit diesem die Zahl $\eta_1 \cdot \eta_2$ gemeinsam, muß ihm also identisch sein, da, wie bewiesen, dieselbe Gitterzahl nicht verschiedenen Gittern angehört. Da nun die Regeln für die Zusammensetzung der Gitter mit denjenigen für die Zusammensetzung der Klassen übereinstimmen, demnach das Produkt zweier konjugierter Gitter gleich dem Hauptgitter ist, und umgekehrt zwei Gitter, welche miteinander zusammengesetzt das Hauptgitter ergeben, zueinander konjugiert sein müssen, findet sich sogleich, daß das zu Γ konjugierte Gitter Γ' gleich dem Produkte $\Gamma_1' \cdot \Gamma_2'$ der zu Γ_1, Γ_2 konjugierten Gitter ist. Aus der Bildungsweise eines Gitterproduktes folgt hiernach

$$\eta \cdot \Gamma' = \eta \cdot \Gamma_1' \Gamma_2' = \eta_1 \eta_2 \cdot \Gamma_1' \Gamma_2' = \eta_1 \Gamma_1' \cdot \eta_2 \Gamma_2',$$

und daraus geht die Gleichung (44) hervor.

Nun sei ε eine Einheit in $\mathfrak{G}$ und $\eta = \eta_1 \cdot \varepsilon$; dann folgt sogleich

$$j(\eta) = j(\eta_1 \cdot \varepsilon) = j(\eta_1) \cdot j(\varepsilon) = j(\eta_1) \cdot \mathfrak{g}$$

und, da ein Ideal durch Multiplikation mit $\mathfrak{g}$ unverändert bleibt, $j(\eta) = j(\eta_1)$; assoziierte Gitterzahlen erzeugen also dasselbe Ideal. Umgekehrt, wenn η, η_1 zwei zu den Gittern Γ, Γ_1 resp. gehörige Zahlen und die von ihnen erzeugten Ideale $j(\eta)$, $j(\eta_1)$, d. h. die Gesamtheiten der Zahlen in $\eta \cdot \Gamma'$ und $\eta_1 \cdot \Gamma_1'$ einander gleich sind, so folgt auch, daß

$$\eta \cdot \Gamma \Gamma' = \eta_1 \cdot \Gamma \Gamma_1',$$

d. h.

$$\mathfrak{g} \eta = \eta_1 \cdot \Gamma \Gamma_1'$$

und somit gewiß η durch η_1 teilbar, $\eta = \eta_1 \cdot \alpha$ ist, wo α eine Gitterzahl; ebenso aber folgt auch η_1 teilbar durch η, $\eta_1 = \eta \cdot \beta$, wo auch β eine Gitterzahl, demnach ist $\eta = \eta \cdot \alpha \beta$, wo auch $\alpha \beta$ eine Gitterzahl sein wird (Nr. 9); da sich hieraus aber $N(\alpha \beta) = 1$ ergibt, sind mit $\alpha \beta$ auch α, β Teiler der Eins d. h. Einheiten in $\mathfrak{G}$ und demnach η, η_1 assoziiert.

13. Eine Folge dieser Resultate ist die Erkenntnis, daß die Teilbarkeit einer Gitterzahl η durch eine andere Gitterzahl η_1 vollkommen identisch ist mit der Teilbarkeit des aus η erzeugten Ideals durch das aus η_1

erzeugte Ideal. Denn einerseits folgt aus der ersteren, d. i. aus einer Gleichung

$$\eta = \eta_1 \cdot \eta_2 ,$$

in welcher auch η_2 eine Gitterzahl ist, nach dem **Satze** voriger Nummer die Gleichung (44), d. i. die behauptete Teilbarkeit der Ideale. Andererseits besteht, wenn das aus η erzeugte Ideal durch das aus η_1 erzeugte teilbar ist, eine Gleichung

$$(45) \qquad j(\eta) = j(\eta_1) \cdot j(\eta_2) ,$$

wo auch $j(\eta_2)$ ein Ideal ist, dessen erzeugende Gitterzahl wir η_2 genannt haben; nach der Übereinstimmung zwischen der Bildung der Zahlen eines Idealproduktes und der Zusammensetzung von Gittern läßt vorstehende Gleichung sich aber schreiben wie folgt:

$$\eta \cdot \Gamma' = \eta_1 \eta_2 \cdot \Gamma_1' \Gamma_2' ,$$

wenn Γ', Γ_1', Γ_2' die konjugierten derjenigen Gitter bezeichnen, denen die erzeugenden Gitterzahlen angehören, und man findet weiter

$$\eta \cdot \Gamma \Gamma' \quad \text{d. h.} \quad \mathfrak{g}\, \eta = \eta_1 \eta_2 \cdot \Gamma \Gamma_1' \Gamma_2' ,$$

wo das Produkt $\Gamma \Gamma_1' \Gamma_2'$ wieder die Gesamtheit der Zahlen eines Gitters darstellt, woraus η gewiß durch $\eta_1 \eta_2$, a fortiori also auch durch η_1 teilbar hervorgeht.

Nunmehr wollen wir eine Gitterzahl, welche keine von ihr selbst verschiedene Gitterzahl, sie sei denn eine der ihr assoziierten, zum Teiler hat, eine Prim-Gitterzahl oder auch eine ideale Primzahl nennen, wobei jedoch die Benennung „ideal" diejenigen Prim-Gitterzahlen, welche etwa dem Hauptgitter angehören, nicht ausschließen soll. Für solche Zahlen schließen wir aus dem Voraufgehenden den **Satz:**

Die idealen Primzahlen der Gesamtheit $\mathfrak{G}$ sind diejenigen ihrer Zahlen, welche Primideale erzeugen. In der Tat: ist $j(\eta)$ ein Primideal, so muß auch η eine ideale Primzahl sein, denn, wäre η zusammengesetzt, bestünde also eine Gleichung $\eta = \eta_1 \cdot \eta_2$, in welcher η_1 eine nicht mit η identische oder assoziierte Gitterzahl bezeichnet, so ginge die Gleichung (44) hervor, der zufolge das Primideal $j(\eta)$ einen davon verschiedenen Idealteiler $j(\eta_1)$ besäße, was unmöglich ist. Ist dagegen $j(\eta)$ kein Primideal, besteht demnach

eine Gleichung (45), in welcher keins der Ideale zur Rechten gleich $\mathfrak{g}$, also keine der Zahlen η_1, η_2 eine Einheit in $\mathfrak{G}$ ist, so ergibt sich, wie dort gezeigt, η teilbar durch $\eta_1 \eta_2$, d. h. gewiß durch eine von ihr verschiedene, ihr auch nicht assoziierte Zahl, und demnach kann auch η keine ideale Primzahl sein.

Wir beweisen endlich diejenige Eigenschaft für die idealen Primzahlen, die stets für Primelemente charakteristisch ist, daß nämlich ein Produkt zweier Zahlen in $\mathfrak{G}$ nur dann durch eine ideale Primzahl teilbar sein kann, wenn es einer seiner Faktoren ist. Wenn π eine ideale Primzahl bedeutet und es besteht eine Gleichung

$$\eta_1 \cdot \eta_2 = \pi \cdot \eta\,,$$

worin η, η_1, η_2 Gitterzahlen bedeuten, so folgt daraus die andere Gleichung

$$j(\eta_1) \cdot j(\eta_2) = j(\pi) \cdot j(\eta)\,,$$

der zufolge nach den für Ideale geltenden Teilbarkeitsregeln einer der Faktoren zur Linken, etwa $j(\eta_1)$ durch das Primideal $j(\pi)$ teilbar sein muß; dann muß aber nach dem im Anfang der Nummer Bewiesenen auch η_1 durch π teilbar sein, w. z. b. w.

14. Durch die nunmehr erhaltenen Sätze sind wir in den Stand gesetzt, für die Zahlen in $\mathfrak{G}$ genau so, wie es für die rationalen ganzen Zahlen sowie für die Ideale der Fall war, ihre eindeutige Zerlegbarkeit in ideale Primfaktoren zu erweisen. Zunächst enthält jede Zahl η in $\mathfrak{G}$ einen idealen Primfaktor π. Ist sie nämlich nicht selbst eine solche Primzahl, so hat sie jedenfalls eine ihr nicht assoziierte Zahl η_1 zum Teiler, so daß $\eta = \eta_1 \cdot \eta^{(1)}$ gesetzt werden kann, während $\eta^{(1)}$ eine Gitterzahl bezeichnet, die keine Einheit in $\mathfrak{G}$ ist, ebenso $\eta_1 = \eta_2 \cdot \eta^{(2)}$, $\eta_2 = \eta_3 \cdot \eta^{(3)}$ usw. fort, solange noch keine der Zahlen $\eta_1, \eta_2, \eta_3, \ldots$ eine ideale Primzahl ist. Dieser Prozeß muß aber nach einer endlichen Anzahl von Schritten endigen, denn aus den erhaltenen Gleichungen folgen diese anderen:

$$j(\eta) = j(\eta_1) \cdot j(\eta^{(1)}) = j(\eta_2) \cdot j(\eta^{(1)}) \cdot j(\eta^{(2)}) = \ldots,$$

in denen die auftretenden Idealfaktoren von $\mathfrak{g}$ verschieden sind und daher nicht in unendlicher Anzahl auftreten können,

da das Ideal $j(\eta)$ nur eine endliche Anzahl von Idealteilern hat. Demnach führt der Prozeß endlich eine Zahl $\eta_k = \pi$ herbei, welche eine ideale Primzahl ist und einen Primteiler von η darstellt.

Setzt man demgemäß $\eta = \pi \cdot \eta_1$, wo η_1 wieder eine Zahl in $\mathfrak{G}$ bezeichnet, so kann auf diese die gleiche Betrachtung angewendet und ein Primteiler π_1 derselben nachgewiesen werden, so daß $\eta_1 = \pi_1 \cdot \eta_2$ gesetzt und nun ebenso weiter geschlossen werden kann. Da aus gleichem Grunde wie vorher auch dieser Prozeß nicht unendlich fortlaufen kann, so erlangt man endlich eine Zerlegung der Zahl η in eine endliche Anzahl von idealen Primfaktoren, d. i. eine Gleichung wie diese:

$$\eta = \pi \cdot \pi_1 \cdot \pi_2 \ldots \pi_\lambda . \tag{46}$$

Der Schlußsatz der vorigen Nummer verstattet aber endlich zu zeigen, daß eine solche Zerlegung der Zahl η in ideale Primfaktoren wesentlich auch nur auf eine einzige Weise möglich ist. Dies geschieht genau wie in der Theorie der rationalen ganzen Zahlen. Wäre nämlich eine zweite Zerlegung

$$\eta = \varkappa \cdot \varkappa_1 \cdot \varkappa_2 \ldots \varkappa_\mu \tag{47}$$

vorhanden, mithin

$$\pi \cdot \pi_1 \ldots \pi_\lambda = \varkappa \cdot \varkappa_1 \ldots \varkappa_\mu , \tag{48}$$

so müßte, da dieser Gleichheit zufolge das Produkt zur Linken durch die ideale Primzahl $\varkappa$ teilbar ist, einer seiner Faktoren, etwa π den Teiler $\varkappa$ haben, der somit, da er keine Einheit und π Primzahl ist, nur mit π assoziiert sein kann; setzt man demgemäß $\varkappa = \pi\varepsilon$, wo ε eine Einheit in $\mathfrak{G}$ bezeichnet, so geht aus der voraufgehenden Gleichung die andere:

$$\pi_1 \pi_2 \ldots \pi_\lambda = \varepsilon \cdot \varkappa_1 \varkappa_2 \ldots \varkappa_\mu$$

hervor, die nun ebenso behandelt werden kann, usw. Man erkennt hieraus allmählich, daß in den beiden Zerlegungen (46) und (47) die Primfaktoren einzeln einander gleich oder doch assoziiert sein müssen und ihre Anzahl also die gleiche ist. Dasselbe folgt aus der Eindeutigkeit der Zerlegung eines Ideals in Primidealfaktoren, wenn man die Gleichung (48) durch die ihr äquivalente:

$$j(\pi) \cdot j(\pi_1) \ldots j(\pi_\lambda) = j(\varkappa) \cdot j(\varkappa_1) \ldots j(\varkappa_\mu)$$

ersetzt. Betrachtet man also zwei Zerlegungen als nicht wesentlich voneinander verschieden, wenn die Faktoren der einen denen der anderen zwar nicht gleich, doch assoziiert sind, so läßt sich folgender **Satz** aussprechen, welcher dem **Fundamentalsatze** von der Zerlegung ganzer Zahlen völlig konform ist:

Jede Zahl der Gesamtheit 𝔊 läßt sich stets und zwar nur auf eine wesentlich eindeutige Weise als ein Produkt idealer Primzahlen dieser Gesamtheit darstellen.

Was von den sämtlichen Zahlen der Gesamtheit 𝔊 gilt, das gilt insbesondere auch für die in ihr enthaltenen ganzen Zahlen des quadratischen Körpers 𝔎: auch diese gestatten eine wesentlich eindeutige Zerlegung in Primfaktoren der gedachten Art, und so sehen wir die Aufgabe, welche schon in Nr. 1 des letzten Kapitels aufgeworfen und in diesem Kapitel wieder aufgenommen worden ist, nunmehr in demselben Sinne gelöst, wie in der rationalen Zahlentheorie. Und doch findet ein wesentlicher Unterschied statt. An der erst angeführten Stelle ist die Tatsache festgestellt, daß eine ganze Zahl γ des quadratischen Körpers 𝔎 nicht stets auf eindeutige Weise in Faktoren zerlegbar ist, die ihrerseits unzerlegbar sind, wenn anders diese Faktoren ebenfalls als ganze Zahlen dieses Körpers gedacht werden; und in der Tat ist der obige Satz nur dadurch von uns erlangt worden, daß wir das Gebiet 𝔤 der ganzen Zahlen des Körpers zum Gebiete 𝔊 aller Gitterzahlen erweiterten und die „idealen Primzahlen" dieses Gebietes als Elemente der Zerlegung der Zahl γ zuließen. Man muß also, wie man zu sagen pflegt, den ganzen Zahlen des Körpers oder den Hauptgitterzahlen die Nebengitterzahlen adjungieren, um die gestörte Gleichmäßigkeit in den Teilbarkeitsgesetzen des quadratischen Körpers wiederherzustellen: der obige Fundamentalsatz besteht für die ganzen Zahlen des quadratischen Körpers nur dann, wenn ideale Primfaktoren eingeführt werden, welche erst die eigentlichen Grundelemente der Zerlegung ausmachen. Doch hat man wohl zu beachten, daß diese idealen Faktoren durchaus nicht bloß ein ungreifbares Imaginäres, sondern in Wirklichkeit existierende ganze algebraische Zahlen sind und nur deshalb den „wirklichen" ganzen Zahlen gegenüber

als „ideal" benannt worden sind, weil sie nicht auch, wie diese, Zahlen des Körpers sind.

Aus der letzten Nummer des vorigen Kapitels entnehmen wir leicht noch endlich den Umstand, daß jede rationale Primzahl p, welche in der Diskriminante D aufgeht, das Quadrat einer idealen Primzahl, jede nicht in D aufgehende Primzahl aber entweder das Produkt aus zwei konjugierten idealen Primzahlen oder selbst als eine solche anzusehen ist, je nachdem die Kongruenz $z^2 \equiv D$ (mod. $4p$) auflösbar ist oder nicht. —

Mit diesen Betrachtungen beschließen wir unser Werk, da mit ihnen die Elemente der Theorie des quadratischen Körpers bzw. der quadratischen Formen in ihren wesentlichen Stücken zur Darstellung gekommen sind. Für die höheren Teile dieser Theorien, die Bestimmung der Anzahl der Ideal- oder Formenklassen, deren Verteilung in Geschlechter und die Anzahl der letzteren u. a. m. sei der Leser auf andere Werke verwiesen, wie u. a. auf *Dirichlet*s Vorlesungen über Zahlentheorie, herausgegeben von *Dedekind*, 4. Aufl. 1894, des Verfassers Analytische Zahlentheorie, 1894, seine Allgemeine Arithmetik der Zahlenkörper, 1905, sowie *Hilbert*s Bericht über die Theorie der Zahlkörper im 4. Jahresberichte der Deutschen Mathematiker-Vereinigung, 1897, endlich auch *J. Sommer*s Vorlesungen über Zahlentheorie, 1907.
